La protection des données à caractère personnel et l'entreprise

Léonard, Thierry

Published in:
Guide juridique de l'entreprise

Publication date:
2007

Document Version
le PDF de l'éditeur

Introduction

010 Gestion de l'information et protection des données

L'information est assurément devenue pour la plupart des entreprises un facteur de production aussi important que le travail, le capital ou l'outil [1]. L'information relative à des personnes physiques est d'une importance stratégique pour les entreprises relevant par exemple du secteur bancaire, de l'assurance ou du marketing. Toutes les entreprises traitent des informations relatives à leur personnel. Elles sont pour la plupart présentes sur le web et utilisent souvent leur site comme un outil de collecte d'informations sur leur clientèle actuelle ou future.

La gestion de ces informations doit respecter un cadre réglementaire de plus en plus touffu et contraignant au sein duquel la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [2] occupe une place de choix.

L'objet de cette législation est par essence « difficile » à appréhender – qui peut par exemple définir avec précision ce qu'est la vie privée? – mais comment alors qualifier la tâche de l'entreprise désireuse d'appliquer en son sein la complexe réglementation issue de son prescrit? C'est d'autant plus vrai que sa mise en œuvre pratique demande une collaboration étroite entre différents acteurs de la vie de l'entreprise: juristes, commerciaux et informaticiens.

020 Législation éparpillée

Les arrêtés royaux d'application de la loi du 8 décembre 1992 n'étaient pas encore tous publiés lorsque l'Union européenne s'est dotée, le 24 octobre 1995, d'une directive relative « *à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* » [3].

La loi du 11 décembre 1998, suivie de son arrêté royal d'application du 13 février 2001 [4], implémente cette directive en droit belge par voie de modifications du texte de la loi initiale. L'arrêté susmentionné simplifie fortement les textes en vigueur en abrogeant la kyrielle d'arrêtés royaux qui exécutaient l'ancienne version de la loi.

L'entreprise soucieuse de respecter la législation sur la protection des données devra cependant rester attentive à l'existence d'autres dispositions pouvant avoir une incidence directe sur son fonctionnement. Ainsi en est-il de certaines dispositions sur

1. E. MEYSMANS, 'De praktische uitvoering van de privacywet in de onderneming', in *Persoonsgegevens en privacybescherming Commentaar op de wet tot bescherming van de persoonlijke levensfeer*, Bruges, Die Keure, 1995, p. 218.
2. Telle que modifié par la loi du 11 décembre 1998. Ci-après dénommée 'la loi'.
3. *J.O.C.E.*, n° L 281, 23 novembre 1995, p. 31 et s.; pour un commentaire approfondi, voir par exemple, M.-H. BOULANGER, C. DE TERWANGNE, Th. LÉONARD *et alii*, 'La protection des données en droit communautaire', *J.T. Eur.*, 1997, pp. 121 à 127, pp. 145 à 155, pp. 173 à 179.
4. Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001, p. 7908 et s. Ci-après dénommé l''arrêté royal'.

le spam, introduites dans la loi sur le commerce électronique [5] ou dans la réglementation du droit du travail [6].

030 Limites de l'analyse

Seules les dispositions de la loi et de son arrêté royal d'exécution pouvant intéresser l'entreprise relevant du secteur privé seront commentées, à l'exclusion des règles spécifiques au secteur public. Les principes protecteurs sont cependant *a priori* identiques [7].

Les dispositions particulières à certains secteurs ne seront pas abordées. On pense essentiellement au chapitre VI de la loi du 12 juin 1991 relative au crédit à la consommation ou aux dispositions propres aux télécommunications.

5. *Cf.* l'article 14 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information et son arrêté royal d'application du 4 avril 2003.
6. Voir par exemple la convention collective n° 81 du 26 avril 2002 rendue obligatoire par arrêté royal du 12 juin 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau (sur ce texte, voir M.-H. Boulanger, A.-Ch. Lacoste, S. Louveaux, 'La surveillance des communications électroniques des employés', *Rev. Ubiquité*, 2003, p. 47 et s.).
7. M.-H. Boulanger, C. De Terwangne, Th. Léonard, 'La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel', *J.T.*, 1993, p. 375, n° 26.

Chapitre 1. Concepts de base et définitions

040 **Importance des définitions**

L'entreprise confrontée à l'application de la loi du 8 décembre 1992 rencontre d'abord une difficulté de compréhension du vocabulaire spécifique et technique retenu par le texte légal.

Les développements des technologies de l'information ont débouché sur un large panel d'outils permettant le traitement de l'information: *Personal Computer*, réseaux informatiques ouverts (intranet) ou fermés, internet, etc. L'entreprise s'est, ce faisant, habituée à manier un certain nombre de concepts désignant tels ou tels technologie ou support utilisés: CD-ROM, disquette, puce électronique, etc.

La loi a voulu réglementer l'ensemble des traitements de l'information sans distinguer selon la technique utilisée. Elle passe dès lors par des notions abstraites recouvrant tout ou partie des technologies intégrées dans l'environnement journalier de l'entreprise.

Il est capital, pour la bonne compréhension de la loi, de s'éloigner de cette réalité technique sous peine d'avoir une idée erronée de son champ d'application.

Les concepts de données, de traitements ou de fichiers reçoivent une définition différente de celle retenue en informatique ou dans le langage courant.

Les définitions de responsable du traitement et de sous-traitant permettent de déterminer la personne morale ou physique destinataire des obligations légales. Enfin, les nouvelles dispositions légales précisent les notions de tiers, de destinataire et de consentement de la personne concernée.

SECTION 1. LA DONNÉE À CARACTÈRE PERSONNEL

050 **Définition – commentaires**

L'article 1er, § 1er de la loi énonce d'abord que les données à caractère personnel sont « *toute information concernant une personne physique identifiée ou identifiable* ».

Si la loi ne définit pas la notion même de « donnée », les travaux préparatoires laissaient déjà entendre qu'une « donnée » ne vise pas seulement une information écrite ou chiffrée mais aussi l'information contenue dans une image, une bande son, ou une empreinte digitale [8].

Toute information est donc susceptible d'être une donnée au sens de la loi, quels que soient sa forme, son sens ou son objet, sous réserve de son caractère personnel [9].

8. Dans le même sens, voir la déclaration d'un membre de la Commission de la vie privée (*in* Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sénat, sess. extr. 1991-1992, no 445-2, p. 19) ainsi que la réponse du Ministre (*idem*, p. 57).
9. M.-H. Boulanger, C. De Terwangne et Th. Léonard, 'La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel', *op. cit.*, p. 371, no 5; D. De Bot, *Verwerking van persoonsgegevens*, Anvers, Kluwer, 2001, p. 23, no 28 et s.

Pour tomber sous le champ d'application de la loi, l'information doit en effet permettre l'identification d'une personne physique [10]. Les personnes morales sont donc exclues de la protection légale. Les traitements relatifs à des entreprises –fichiers « business to business », etc. – sont toutefois visés dès lors qu'ils contiennent de l'information sur des personnes physiques (p. ex.: les noms des administrateurs d'une société ou des membres d'une association sans but lucratif) [11].

La nouvelle version de la définition apporte cependant une précision importante. Reprenant textuellement la directive qui la fonde, elle répute comme identifiable: « *une personne qui peut être identifiée directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ».

Un numéro de téléphone, de plaque d'immatriculation de voiture, de sécurité sociale ou de passeport peut ainsi être considéré comme une donnée à caractère personnel.

L'exposé des motifs de la nouvelle loi interprète très largement le caractère identifiable de la donnée [12]. Dès lors qu'il existe un moyen raisonnable d'identifier les personnes concernées, soit dans le chef du responsable du traitement, soit même par un tiers, il s'agit d'une donnée à caractère personnel dont le traitement est susceptible d'être réglementé par la loi. Cette interprétation a fait l'objet de différentes critiques dès lors qu'elle impose l'application de la loi à des responsables incapables d'identifier les personnes concernées par les données traitées [13].

---

10. Jugé que les héritiers et ayants droit doivent être assimilés à la personne concernée au sens de la loi (Civ. Bruxelles (2e ch.), 23 avril 1999, *Rev. Dr. Santé*, 1999-2000, p. 353 et s. et note M.-H. Boulanger). La loi serait donc susceptible de s'appliquer aux personnes physiques décédées dans certaines hypothèses. En l'espèce, il s'agissait de données médicales relatives à une personne décédée dont l'époux demandait la transmission à un médecin. Sur ce point, voir D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 26 ainsi que l'avis de la Commission de la protection de la vie privée n° 18/2000 du 15 juin 2000 relatif au droit d'accès des héritiers au dossier médical du défunt qui en appelle à une réglementation *ad hoc* vu l'incertitude juridique qui entoure la reconnaissance de la protection des informations relatives à la personne décédée, http://www.privacy.fgov.
11. De manière assez étonnante, la Commission de la protection de la vie privée a considéré notamment que dans le cadre du répertoire national des personnes morales et des groupements dénués de la personnalité juridique, les S.P.R.L. unipersonnelles et les associations de fait constituées de différentes personnes physiques identifiables devaient être considérées '*dans le prolongement de leur qualité de personnes morales ou de groupements dénués de la personnalité juridique*'. En conséquence, selon elle, ces informations ne devaient pas être considérées comme des données à caractère personnel (avis n° 26/1999 du 25 août 1999 relatif à un projet de loi organisant un répertoire national des personnes morales et des groupements dénués de la personnalité juridique, soumis à des obligations ou titulaires de droits en vertu de la législation fiscale, sociale ou économique belge, http://www.privacy.fgov.be).
12. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 12, notamment: '*Une information relative à une personne est donc considérée comme donnée à caractère personnel tant que quelqu'un est encore en mesure, par quelque moyen qui puisse raisonnablement être mis en œuvre, de déterminer à quel individu se rapporte cette information. Sont donc également considérées comme 'données à caractère personnel' les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne*'.
13. Voir par exemple, D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 29 et s., nos 35 à 39; Th. Léonard et Y. Poullet, 'La protection des données à caractère personnel en pleine (r)évolution', *J.T.*, 1999, p. 378, n° 3. Pour des exemples d'application de l'interprétation large, voir par exemple, C.E., 26 janvier 2000, A.S.B.L. Fédération belge des chambres syndicales des médecins et autres, n° 84880, *Rev. Dr. Santé*, 2000-2001, p. 285 et s. et note S. Callens (à propos du résumé psychiatrique minimum) et avis de la Commission de la vie privé n° 34/2001 du 22 novembre 2000 relatif à la protection de la vie privée dans le cadre du commerce électronique concernant les adresses IP des internautes (http://www.privacy.fgov.be). Pour une analyse de ces deux interprétations, Y. Poullet, A. Cruquenaire, N. Daubies *et alii*, *Droit de l'informatique et des technologies de l'information Chronique de jurisprudence 1995-2001*, Bruxelles, Larcier, 2003, p. 140, n° 146 et s.

060 **Protection des données et protection de la vie privée**

Le fondement de l'intervention législative est maintenant indiqué à l'article 2 de la loi: «*Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée*».

Il ne s'agit pas seulement de protéger la vie privée des individus. C'est en effet l'ensemble des libertés et droits fondamentaux des personnes physiques qui peuvent être énervés lors de traitements de données à caractère personnel. On retrouve ici l'idée d'un élargissement de la protection traditionnelle en matière de protection de la vie privée [14]. *A priori*, aucune distinction n'est à opérer suivant le caractère public ou privé de l'information: tout traitement de donnée à caractère personnel tombe sous le champ d'application de la protection, qu'il révèle ou non une ingérence dans la vie privée de l'individu.

Des données ayant trait aux activités commerciales ou professionnelles de personnes physiques tombent normalement sous le champ d'application de la loi [15], sauf application d'une exception légale.

SECTION 2. LE TRAITEMENT

070 **Concept bicéphale**

Au sens de la loi, le traitement couvre tant celui opéré par des procédés automatisés que celui qui est indépendant de tels procédés.

Le traitement peut donc être automatisé ou non. Mais les obligations légales diffèrent dans les deux cas. Si le traitement n'est pas automatisé les données doivent être contenues dans un fichier au sens où la loi le définit pour que la protection légale trouve à s'appliquer.

SOUS-SECTION 1. LE TRAITEMENT AUTOMATISÉ DE DONNÉES

080 **Définition – Conditions**

L'article 1er, § 2 de la loi définit le traitement comme: «*toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel*».

Pour qu'il y ait traitement automatisé, deux conditions doivent donc être remplies: l'existence d'une ou plusieurs opérations effectuées sur les données et l'utilisation de procédés automatisés. A notre sens, un élément supplémentaire doit être retenu: une finalité d'utilisation transcendant toute utilisation des données.

---

14. Voir sur ce point, Th. LÉONARD, Observations sous Civ. Bruxelles, Prés., 22 mars 1994, *J.T.*, 1994, pp. 849 et 850. Dans le même sens, D. DE BOT, *Verwerking van persoonsgegevens*, *op. cit.*, p. 35, no 40.
15. Civ. Bruxelles (Prés.), 22 mars 1994, *J.T.*, 1994, p. 843; Civ. Nivelles (Prés.), 15 novembre 1994, *J.T.*, 1995, p. 284; J.-P. BUYLE, L. LANOYE, Y. POULLET et V. WILLEMS, 'Chronique de jurisprudence L'informatique (1987-1994)', *J.T.*, 1996, p. 231, no 57.

090 Existence d'opérations effectuées sur les données

Une ou plusieurs opérations doivent être effectuées sur les données. Le texte en prévoit de différents types: la collecte, l'enregistrement, la conservation, la modification, l'effacement, la consultation, etc.

Contrairement à l'ancien texte, une seule opération suffit pour appeler l'application matérielle de la loi. Ainsi, le simple captage et visionnage d'images [16], la simple consultation d'une banque de données en ligne ou d'une page web sur internet pourraient bien impliquer une application intégrale de la loi dans le chef de celui qui visionne ou consulte les informations qui y sont contenues [17]. Cette conception a déjà été amplement critiquée [18]. Quel est en effet le sens à donner à l'obligation d'informer la personne concernée ou à l'obligation de notification auprès de la Commission de la protection de la vie privée si les données consultées ne font l'objet d'aucune conservation ou enregistrement dans le chef du consultant?

100 Utilisation de procédés automatisés

Les opérations doivent être effectuées en tout ou en partie à l'aide de procédés automatisés. La notion de procédé automatisé est extrêmement vague, ce qui permet d'englober à peu près toutes les nouvelles technologies de l'information (informatique, télématique, réseaux de télécommunication, etc.).

Il est nécessaire, mais suffisant, qu'à un moment de la procédure de traitement de l'information intervienne un procédé automatisé pour que l'ensemble des opérations constitue un traitement automatisé au sens de la loi. Si des fiches papiers sont classées suivant des numéros d'identification repris ensuite dans la mémoire d'un ordinateur – ce qui facilite la recherche des fiches – l'ensemble du traitement devra donc être réputé automatisé. Il en est de même pour une communication d'informations sur papier imprimé grâce au logiciel qui gère une banque de données.

Le procédé automatisé dont il est question vise l'emploi d'une machine « intelligente » pour effectuer des opérations sur les données. Ces dernières sont possibles sans intervention humaine. L'utilisation d'une photocopieuse ou d'un fax ne sont pas des procédés automatisés au sens de la loi. La machine ne peut effectuer seule des opérations sur l'information copiée [19]. Un ordinateur, par contre, grâce à ses logiciels, saisit l'information, la trie, en déduit d'autres, etc.

110 Opération(s) effectuée(s) en vue de la réalisation d'une ou plusieurs finalités

Toute personne désireuse de se conformer à la loi bute d'emblée sur une difficulté: comment identifier un traitement au sens de la loi ? La question est essentiellement

16. En ce sens, l'avis de la Commission de la vie privée n° 34/1999 du 13 décembre 1999 relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéo-surveillance, http://www.privacy.fgov.be.
17. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 13: '*Une extraction, par exemple, ou une consultation unique d'un fichier contenant des données à caractère personnel constitue également un traitement auquel s'appliquent les dispositions de la loi*'; pour autant que cette opération unique tombe sous le champ d'application territorial de la loi.
18. M.-H. Boulanger, C. De Terwangne, Th. Léonard *et alii*, 'La protection des données en droit communautaire', *op. cit.*, pp. 125 et 126, n° 16; M.-H. Boulanger, C. de Terwangne, 'Internet et le respect de la vie privée', in *Internet face au droit*, Diegem-Namur, Story Scientia-C.R.I.D., Cahiers du C.R.I.D., n° 12, 1997, pp. 198 et 199.
19. Dans le même sens, D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 64, n° 91.

pratique. La détermination des différents traitements est la première étape indispensable à son application au sein de l'entreprise du responsable du traitement. En effet, en pratique, tout le contrôle du respect de la loi se fait au niveau de chaque traitement.

Le critère unificateur des diverses opérations peut encore résider, d'après nous, dans la finalité « générique » poursuivie par le traitement. A chaque traitement correspond une ou un certain nombre d'opérations participant toutes à la réalisation d'un seul et même but [20]. S'il est vrai que cette unification conceptuelle (un traitement = une finalité d'utilisation des données) n'est plus nécessaire au vu de la définition légale [21], elle ne heurte pas la protection mise en place [22]. Du reste, même ceux qui critiquent cette assimilation admettent que le contrôle de l'application du principe de finalité doit encore s'effectuer finalité par finalité. Notre approche présente par contre, selon nous, l'avantage d'offrir un critère précis de détermination du traitement permettant tant une protection optimale de l'individu [23] qu'une limitation du risque juridique dans le chef du responsable du traitement [24].

Ainsi, si une entreprise effectue une série d'opérations sur les données de son personnel en vue du paiement de leur rémunération, l'enregistrement des données, mais aussi leur rapprochement (p. ex. le rassemblement de toutes les sommes versées à un individu durant une période déterminée), voire leur diffusion limitée (envoi des fiches de salaires, envoi de données aux organismes de sécurité sociale), constituent des applications poursuivies en vue de la réalisation d'une seule et même finalité: le paiement des rémunérations du personnel.

Par conséquent, la finalité peut parfaitement servir de critère de distinction des traitements entre eux. Le critère n'est pas ici matériel – par exemple le support – mais abstrait – le but d'utilisation des données –. Une même banque de données peut révéler différents traitements automatisés au sens où nous l'entendons, même si l'on peut n'y voir qu'un traitement au sens de la définition légale.

Une banque de données clientèle peut par exemple être utilisée pour la gestion du service proposé au client mais aussi pour effectuer des opérations de marketing. Un traitement peut certes viser plusieurs finalités de marketing. On pourrait dès lors

20. Dans le même sens mais sous l'ancienne loi, S. GUTWIRTH, 'De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens', *T.P.R.*, 1993, p. 1460, n° 29; M.-H. BOULANGER, C. DE TERWANGNE, Th. LÉONARD, 'La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel', *op. cit.*, p. 372, n° 9; J. DUMORTIER, Fr. ROBBEN, note sous Comm. Anvers, 7 juillet 1994 et Comm. Bruxelles, 15 septembre 1994, *Computerrecht*, 1994, p. 248; Th. LÉONARD, Y. POULLET, 'Fichiers bancaires: de quelques questions de vie privée', in *Financieel Recht tussen Oud en Nieuw*, Anvers, Maklu, 1996, pp. 557 et 558.
21. Et nous sommes entièrement d'accord avec M. DE BOT lorsqu'il énonce que l'application matérielle de la loi est indépendante de la finalité visée par le traitement (D. DE BOT, *Verwerking van persoonsgegevens*, *op. cit.*, p. 38 n^os 43 et 44). Notre souci est ici beaucoup plus terre à terre: ne pas nous départir d'une règle d'identification des traitements simple permettant l'application logique et systématique des règles (trop) complexes prévues par la loi.
22. Elle ne réduit pas, par exemple, le champ d'application matériel de la loi même si, nous l'admettons, l'existence d'une finalité n'est pas nécessaire à l'application de la loi. Il n'empêche que tout traitement de données est normalement traversé par une finalité d'utilisation, fût-elle indéterminée.
23. Plus la finalité est déterminée de manière précise, plus la protection découlant du principe de finalité est efficace.
24. Si, d'emblée, une entreprise définit trop largement ses traitements en ne distinguant pas ceux-ci suffisamment au regard des finalités poursuivies, elle risque fort d'appliquer erronément le principe de finalité à des buts d'utilisation trop larges. Nous verrons que de telles approches ont précisément déjà été censurées par les tribunaux (*cf. infra*, n° 300). Par contre, si elle adopte dès le départ une approche par des finalités très précises correspondant chacune à un seul et même traitement, elle réduit fortement le risque de censure.

s'arrêter à cette définition. Mais ne pas définir plus précisément la finalité de départ peut réserver de mauvaises surprises par la suite. Il a ainsi été jugé que la promotion et la prospection de produits financiers d'une banque participaient à une finalité distincte du marketing de produits d'assurance [25]. On voit ici tout le risque d'une définition du traitement indépendante des finalités poursuivies: une fois le traitement identifié, tout porte à croire que l'entreprise raisonnera au départ de l'ensemble des finalités du traitement sans plus tenter par la suite de préciser chacune des finalités qui y seraient artificiellement regroupées.

Sous-section 2. Le traitement non automatisé

120 Définition – Conditions

De la définition du traitement se déduit l'existence légale du traitement non automatisé. Ce dernier ne tombe toutefois sous le champ d'application de la loi que si le traitement porte sur des données « *contenues ou appelées à figurer dans un fichier* » [26].

Pour qu'il y ait un traitement non automatisé, trois conditions doivent être remplies: l'existence d'une ou plusieurs opérations sur les données (1), l'existence d'un fichier (2) et l'utilisation exclusive de procédés non automatisés (3).

La première de ces conditions ayant déjà été examinée, on se limitera à l'analyse des deux autres.

130 Existence d'un fichier – Exclusion des dossiers

L'article 1er, § 2 définit aujourd'hui le fichier comme « *tout ensemble de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* ».

Au sens le plus classique du terme, le fichier désigne un simple ensemble de données traitées en vue d'une utilisation particulière. En subordonnant l'existence du fichier à une condition expresse d'accessibilité des données, la loi vise à exclure les dossiers de son champ d'application.

Le critère retenu est précisé par rapport à l'ancienne loi. La structure des données à caractère personnel doit permettre leur accessibilité selon des critères déterminés. Ce n'est donc pas les dossiers eux-mêmes qui doivent faire l'objet d'une organisation ou structuration mais bien les données qu'ils contiennent en vue d'en faciliter l'accès et l'utilisation [27] . La nouvelle loi est cependant muette concernant le niveau d'accessibilité à atteindre pour admettre la qualification de fichier. On peut donc s'attendre à ce que les difficultés d'application de cette notion continuent [28].

---

25. Comm. Anvers (Prés.), 7 juillet 1994, *D.C.C.R.*, 1994, p. 83 et note de Th. Léonard confirmée par Anvers (5e ch.), 13 mai 1999, *A.J.T.*, 1999-2000, p. 437 et s.
26. Art. 3, § 1er de la loi.
27. Le considérant 27 de la directive précise bien que '*les dossiers ou ensemble de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive*'. Dans le même sens, Y. Poullet, A. Cruquenaire, N. Daubies *et alii*, *Droit de l'informatique et des technologies de l'information Chronique de jurisprudence 1995-2001*, *op. cit.*, p. 143, no 147.
28. Il est significatif que la seule affaire belge ayant donné lieu, en la matière, à un arrêt de la Cour de cassation ait précisément porté sur la définition du '*fichier*' (voir Cass. (1re ch.), 16 mai 1997, *J.T.*, 1997, p. 779).

La Commission de la protection de la vie privée a toujours opté pour une définition très large de la notion de fichier [29]. La jurisprudence est, quant à elle, plus restrictive bien qu'il ne paraisse pas possible de préciser le critère de distinction retenu, l'analyse gisant presque intégralement en fait [30].

Contrairement à ce que soutient un arrêt de la Cour d'appel d'Anvers, la loi s'applique même lorsque le fichier n'est pas conçu pour être conservé durant une longue période [31]. Il s'agissait en l'espèce d'une demande d'accès, introduite par la personne concernée, à un dossier de candidature constitué par le Ministère de la Justice en vue de pourvoir une place vacante de président d'un tribunal. La Cour d'appel a considéré que le dossier en cause, de par sa nature « occasionnelle » – il ne devait être consulté que durant la période d'examen des candidatures – ne permettait pas une consultation systématique des données. Ce faisant, elle ajoutait une condition relative à la durée de la conservation, absente de l'ancienne définition légale du fichier et contraire au nouveau texte puisque, dorénavant, un traitement peut exister indépendamment de toute condition de conservation des données.

140 Utilisation d'un procédé non automatisé

Les données doivent être conservées et utilisées sur un support non automatisé. A l'opposé de la définition des traitements automatisés, on vise ici les utilisations de données qui ne s'effectuent pas par le biais d'une technologie de l'information « avancée » (informatique, télématique, etc.). On pense à toute technique qui ne nécessite pas l'emploi d'une machine « intelligente » pour effectuer des opérations sur les données. En ce sens, le support permet un accès direct de l'opérateur à l'information et ce, de manière autonome (la feuille de papier, la microfiche [32], la cassette analogique, etc.).

SECTION 3. LE RESPONSABLE DU TRAITEMENT ET LE SOUS-TRAITANT

150 Définition du responsable du traitement

Les concepts de « *maître du fichier* » et de « *gestionnaire du traitement* » ont été remplacés par les définitions de « *responsable du traitement* » et de « *sous-traitant* ».

L'article 1er, § 4 de la loi définit le responsable du traitement comme « *la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou*

29. *Cf.* par exemple, avis de la Commission de la protection de la vie privée n° 15/2000 du 24 mai 2000, http://www.privacy.fgov.be où elle estime que des archives conservées 'en bon ordre' qui contiennent des données à caractère personnel doivent être considérées comme des fichiers tout en insistant sur le fait que l'admission ou le rejet de la qualification dépend d'une analyse *in concreto* du contenu et de la manière dont les archives sont conservées; avis n° 21/1998 du 27 juillet 1998 relatif à un avant-projet de loi modifiant la loi sur les hôpitaux concernant les dossiers médicaux, http://privacy.fgov.be.
30. Voir par exemple, Civ. Hasselt (réf.), 2 octobre 1997, *Rev. Dr. Santé*, 1997-1998, p. 333 et s. et note W. VERCRUYSSEN (ancienne définition; refus de la qualification de dossiers médicaux); Trib. trav. Gand (4e ch.), 1er octobre 1999, *T.G.R.*, 2000, p. 90 et s.; *A.J.T.*, 1999-2000, p. 850 et s. (ancienne définition; refus de la qualification d'une liste d'envois postaux à des assurés sociaux); Bruxelles (1re ch.), 14 septembre 1999, *A.M.*, 2000, p. 93 et s. (ancienne définition; refus de qualification concernant la publication d'un nom et de l'âge d'une personne dans un magazine).
31. Anvers (1re ch.), 27 septembre 1995, *A.J.T.*, 1995-96, note J. DUMORTIER; *R.W.,* 1995-1996, p.750.
32. Certes, dans ce cas, l'utilisation d'une 'machine' est nécessaire pour accéder à l'information. Ce procédé ne peut cependant pas être considéré comme un support automatisé; il consiste en une simple loupe mais ne permet pas en lui-même de traiter les données.

conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel (...) »[33].

Si le critère de la détermination des finalités est conservé, celui de la détermination des « *moyens* » du traitement remplace celui du choix des catégories de données, présent dans l'ancienne loi. Les deux critères sont dorénavant cumulatifs.

La définition légale précise que la prise de décision quant aux finalités et moyens du traitement peut être conjointe, ce qui impliquera alors l'identification de plusieurs responsables à l'égard d'un même traitement. Ainsi, si différents opérateurs de télécommunication centralisent des données relatives aux abonnés présentant des retards de paiement, ils seront chacun considérés comme responsable du traitement centralisé. Par contre, s'ils se groupent en une entité juridique distincte, cette dernière apparaîtra comme le responsable des divers traitements de données créés en son sein. On peut aussi penser aux centrales de crédit ou de risques particuliers en matière d'assurance.

Cette nouvelle définition peut poser, en pratique, pas mal de difficultés lorsqu'il s'agit de déterminer qui est le responsable du traitement au sein de groupes d'entreprises, soit parce que des entités juridiques distinctes déterminent les finalités et les moyens du traitement, soit parce que le traitement est mis à la disposition de plusieurs entreprises du groupe par une seule entité[34].

160 Définition du sous-traitant

Celui qui traite les données pour le compte du responsable est désigné par le terme de « *sous-traitant* »[35].

Il peut s'agir du prestataire informatique qui gère le traitement, de l'entreprise de marketing direct qui met à jour les données de ses clients, du secrétariat social qui gère le paiement des salaires pour une P.M.E., etc.

Le sous-traitant doit être distingué de celui qui traite les données sous l'autorité directe du responsable, à savoir principalement le préposé ou le fonctionnaire agissant dans le cadre de leur contrat de travail ou statut.

170 Responsable du traitement et sous-traitant – Distinction

Dans un certain nombre de situations, il n'est pas aisé de distinguer le responsable du traitement et le sous-traitant. On pense par exemple à l'employeur qui confie, en tout ou partie, la gestion de l'administration du personnel à un secrétariat social ou à une autre entreprise de service équivalente ou encore à l'entreprise qui fait appel à une société de marketing direct aux fins de déterminer un public ciblé pour une de ses campagnes publicitaires.

En théorie, des distinctions devraient être opérées suivant les critères légaux d'identification du responsable du traitement. Le prestataire de service qui traite

33. La définition légale se poursuit en indiquant que: '*Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance*'.
34. Pour une analyse plus fouillée, D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 46 et s., n^os^ 60 à 63.
35. Article 1^er^, § 5 de la loi: '*la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données*'.

des données de son client dans le cadre des services prestés devra généralement être considéré comme un responsable du traitement. Si un secrétariat social, contacté par un employeur, assure le paiement des salaires, ainsi que les différentes obligations administratives liées, se dote d'un outil informatique performant lui permettant de traiter toutes les informations nécessaires, il paraît seul décider de sa finalité et des moyens du traitement. Il en est de même pour la société de marketing direct qui, à partir de ses propres banques de données, fournit une liste d'adresses ciblées à ses clients.

En pratique, les situations sont toutefois plus complexes. Celui qui fait appel à un prestataire de services peut aussi vouloir garder le contrôle de toutes les informations qu'il lui transmet. Il est donc recommandé aux parties de déterminer avec précision dans leur contrat, quelles sont les qualités de chaque partie au regard de la loi. On peut d'ailleurs imaginer que les différentes obligations soient partagées entre parties.

SECTION 4. AUTRES DÉFINITIONS

180 Tiers et destinataire

La notion de « *tiers* » [36] fait dorénavant l'objet d'une définition légale. Il s'agit de toute autre personne que le responsable du traitement, le sous-traitant et les personnes qui traitent les données sous leur autorité directe. La plupart du temps, deux sociétés du même groupe d'entreprises sont ainsi tiers au sens de la loi.

Le concept de « *destinataire* » est tout à fait neuf [37]. Proche de la notion de « *tiers* » en ce qu'il vise les personnes qui reçoivent communication des données, il s'en distingue cependant par le fait que ces personnes peuvent faire partie de l'entité du responsable du traitement ou du sous-traitant. On vise donc par là, outre la communication à des tiers au sens précité, les flux d'informations entre départements d'une même société [38]. Cette notion est principalement utilisée dans le cadre de l'obligation d'information qui oblige notamment le responsable du traitement à informer la personne concernée des destinataires de données.

190 Consentement de la personne concernée

La loi définit enfin ce qu'il faut entendre par le « *consentement de la personne concernée* ». Le consentement de la personne concernée joue un rôle essentiel dans la protection mise en place. Il permet par exemple de légitimer un traitement ou de lever l'interdiction de traitement des données sensibles. La loi vise par là « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* » [39].

36. Article 1er, § 6 de la loi: '*la personne physique, la personne morale, l'association de fait ou l'administration publique, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données*'.
37. Article 1er, § 7 de la loi: '*la personne physique, la personne morale, l'association de fait ou l'administration publique qui reçoit communication de données, qu'il s'agisse ou non d'un tiers (...)*'; cette disposition précise en outre que '*les instances administratives ou judiciaires qui sont susceptibles de recevoir communication de données dans le cadre d'une enquête particulière ne sont toutefois pas considérées comme des destinataires*'.
38. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, no 1566/1, p. 16.
39. Article 1er, § 8 de la loi.

Toute manifestation de volonté peut constituer un consentement. Il ne doit pas nécessairement être donné par écrit et peut être implicite, sauf exception prévue par la loi [40].

Le consentement doit être libre, c'est-à-dire être donné en dehors de toute pression. L'idée est de prévenir toute menace de discrimination suite au choix de la personne concernée. Cette condition paraît bien illusoire en pratique. La pression économique consistant dans le risque de se voir refuser un produit ou un service considéré à tort ou à raison comme essentiel par la personne concernée l'amènera bien souvent à donner son consentement sans aucun esprit critique.

Le consentement doit également être spécifique. Il ne peut avoir un objet général mais doit porter sur des traitements précisément définis notamment en leurs finalités, poursuivis par des responsables déterminés.

Le consentement doit enfin être informé. Le responsable du traitement doit donc transmettre à la personne concernée toute information nécessaire à l'analyse du risque particulier que représente le traitement envisagé pour ses droits et libertés. A cet égard, l'information reçue par la personne concernée au moment de la collecte semble constituer un minimum.

40. Par exemple en matière de données dites sensibles (*cf. infra*, n° 360 et s.).

Chapitre 2. Champ d'application

SECTION 1. CHAMP D'APPLICATION MATÉRIEL

200 Principe

Le champ d'application *ratione materiae* de la loi est particulièrement vaste. Elle s'applique à tout traitement de données à caractère personnel dès lors qu'il est automatisé en tout ou partie. Elle s'applique également aux traitements non automatisés de données contenues ou destinées à figurer dans un fichier.

L'article 3, § 2 prévoit cependant différentes exceptions ne bénéficiant pour la plupart qu'aux entités relevant du secteur public. Deux exceptions au champ d'application matériel retiennent néanmoins ici brièvement notre attention [41].

210 Première exception: traitements dans l'exercice d'activités personnelles ou domestiques

L'article 3, § 2 de la loi exclut de son champ d'application le « *traitement de données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques* ».

Seuls les traitements tenus à titre personnel ou domestique par des personnes physiques sont visés. On peut penser aux traitements poursuivis aux fins de la gestion du budget familial, les répertoires d'adresses privés, l'organisation d'événements privés comme un mariage, etc.

Les sociétés ou associations ne bénéficient jamais de cette exception, au contraire des personnes physiques qui la composent. A partir du moment où ces traitements sont mis en œuvre, même occasionnellement, à titre professionnel ou public, ils tombent dans le champ de la loi. Ainsi, le courtier d'assurance qui s'adresse à des connaissances afin de leur proposer une police d'assurance doit respecter la loi même s'il se base sur son répertoire d'adresses privé.

220 Seconde exception: traitements effectués aux seules fins de journalisme ou d'expression artistique ou littéraire

L'article 3, § 3 de la loi exclut partiellement de son champ d'application les traitements effectués aux seules fins de journalisme ou d'expression artistique ou littéraire. Le but était ici de se conformer à l'article 9 de la directive qui imposait aux Etats membres de prévoir des exemptions et dérogations aux principes fondamentaux de la protection « *dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression* ».

41. Notons que l'article 3, § 5, 4° de la loi énonce que les dispositions relatives à l'obligation d'information, au droit d'accès et au droit de correction (art. 9, 10, § 1er et 12) ne s'appliquent pas aux traitements de données à caractère personnel rendus nécessaires par la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux.

Il ne peut être question ici de commenter en détail une disposition qui demanderait à elle seule une étude approfondie [42]. Retenons ici qu'au nom des libertés d'expression et artistiques, des exceptions conditionnées sont reconnues à la protection légale mise en place concernant principalement le régime des données sensibles, à l'obligation d'information, aux droits d'accès et de correction ainsi qu'à l'obligation de déclaration.

SECTION 2. CHAMP D'APPLICATION TERRITORIAL

230 **Principe**

La loi, en son article 3*bis*, prévoit deux critères de rattachement permettant d'appeler à la protection légale.

Pour que la loi belge soit applicable, il faut:

– soit que le traitement soit « *effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public* »;
– soit, si le responsable du traitement n'a pas d'établissement sur le territoire de la Communauté européenne, que ce dernier « *recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge* » [43].

240 **Hypothèse d'un établissement fixe du responsable sur le territoire belge**

Le traitement doit être effectué *dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement.* C'est donc la loi du territoire sur lequel se situe l'établissement pour lequel le traitement est effectué qui est applicable [44].

Ainsi, une entreprise étrangère qui effectue un traitement sur son territoire ne sera pas soumise à la loi belge si, malgré la présence de filiales sur le territoire belge, le traitement n'est pas poursuivi dans le cadre des activités de cette filiale. On peut par exemple penser à des traitements poursuivis dans le cadre d'un site web ouvert par la maison mère étrangère d'un groupe de sociétés dont une filiale se situe en Belgique, pour autant que les services qui sont prestés via ce site le sont par la seule maison mère, indépendamment de sa filiale belge. Ainsi, des commandes de disques peuvent être effectuées sur le web sans intervention d'une filiale située en Belgique. Le

42. Voir notamment, concernant l'ancienne loi même si les questions fondamentales abordées restent d'actualité M. Flamée et Th. Léonard, 'La liberté de la presse à l'aune de la protection des données: liberté responsable ou liberté surveillée?', *Revue Générale de Droit Civil,* 1997, p.5 à 42; voir aussi Avis de la Commission de la protection de la vie privée n° 09/95 du 5 avril 1995 concernant l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel par les médias, http://www.privacy.fgov.be; concernant la disposition actuelle, voir D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 74 et s., n^os^ 101 à 110; L. Geûens, 'Presse et vie privée: vraie question de libertés, fausse question de censure', *Rev. Ubiquité*, 1999, p. 67 et s.; Th. Léonard et Y. Poullet, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, p. 380, n^os^ 10 à 14 .
43. Le responsable doit alors désigner un représentant établi sur le territoire belge. Ce dernier assurera le lien nécessaire entre le responsable du traitement situé à l'étranger et les personnes concernées par les données et/ou les autorités de contrôle. Il sera, le cas échéant, responsable du non-respect de la loi sans préjudice d'actions éventuelles intentées contre le responsable lui-même.
44. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 26.

traitement des données poursuivi par la maison mère n'est pas effectué dans le cadre des activités de la filiale belge.

Une autre condition essentielle est, selon nous, contenue dans le critère retenu par la loi belge [45]. L'établissement doit participer au traitement des données dans le cadre de ses activités et n'est soumis à la loi que dans la mesure du traitement qu'il opère sur les données. S'il profite donc de données traitées en dehors du territoire –il a par exemple un accès *on line* à une banque de données organisée à l'étranger par une société sœur – la loi belge ne s'applique à lui que pour les opérations subséquentes de traitement (p. ex., il intègre les données consultées dans sa propre banque de données).

Une dernière condition est que l'établissement du responsable du traitement pour lequel le traitement est effectué soit situé sur le territoire belge.

La loi, reprenant le principe contenu dans la directive, vise tout établissement fixe du responsable du traitement. L'exposé des motifs se réfère expressément au considérant 19 de la directive selon lequel « *l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable* ». Ce considérant précise en outre que « *la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard* ».

250 Hypothèse de l'établissement du responsable situé en dehors du territoire européen

Le responsable du traitement n'a pas d'établissement sur le territoire de la Communauté européenne mais « *recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge* » [46]. La loi belge lui est alors applicable.

La portée exacte de ce critère n'est pas claire. Il pose en outre d'inextricables difficultés dans son éventuelle application aux traitements poursuivis dans le cadre de la gestion d'un site internet au départ d'un pays tiers à l'Union.

Deux interprétations peuvent, à tout le moins, être défendues [47].

La *première interprétation* consiste à appliquer cette disposition à la lettre. Dès lors que le responsable n'a pas d'établissement sur le territoire communautaire mais utilise n'importe quel moyen [48] situé sur le territoire belge en vue de traiter des données à caractère personnel, la loi belge s'appliquerait sous réserve du seul transit des données sur le territoire.

Il en résulterait un phénomène de rattachement de tout traitement situé en dehors des Communautés aux lois nationales dès lors que ce traitement présenterait un lien matériel, si minime soit-il, avec le territoire d'un pays des Communautés, en l'espèce

---

45. Dans le même sens, D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 91 et s., n° 121; Th. Léonard et Y. Poullet, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, p. 382, n° 19.
46. Le responsable doit alors désigner un représentant établi sur le territoire belge. Ce dernier assurera le lien nécessaire entre le responsable du traitement situé à l'étranger et les personnes concernées par les données et/ou les autorités de contrôle. Il sera, le cas échéant, responsable du non-respect de la loi sans préjudice d'actions éventuelles intentées contre le responsable lui-même.
47. Voir notamment sur cet épineux débat, D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 92 et s., n° 124 et s.; Th. Léonard et Y. Poullet, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, p. 383, n° 20 et s.
48. D'après l'exposé des motifs, '*le terme 'moyens' recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunication, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routers, etc.*' (p. 27).

la Belgique. En conséquence par exemple, tout traitement de données à caractère personnel poursuivi dans le cadre d'un site web dont le responsable est établi dans n'importe quelle partie du monde serait soumis à la loi belge dès lors que ce site permettrait la collecte de ces données par des moyens situés sur le territoire belge – le P.C. du surfeur belge, son logiciel de navigation, les installations de son fournisseur d'accès, les lignes des opérateurs de télécommunication, etc.

Une *deuxième interprétation* prend le contre-pied de la première. La disposition commentée doit se comprendre à la lumière de sa *ratio legis* et des autres dispositions de la loi, principalement celles relatives aux flux de données vers les pays tiers à la Communauté.

Elle amène à retenir l'application de l'article 3*bis*, 2° dans deux catégories de situations [49]. La première est celle où le responsable du traitement cherche délibérément à contourner les lois nationales prises en vertu de la directive et, pour ce faire, délocalise son établissement dans un pays tiers tout en utilisant encore certains moyens sur le territoire communautaire. La seconde vise le cas où le responsable du traitement réalise, par des moyens propres situés sur le territoire européen, un flux de données vers le pays tiers où il traite les données [50].

49. Cette interprétation a été défendue en matière d'Internet par M.-H. BOULANGER, C. DE TERWANGNE, « Internet et le respect de la vie privée », *op. cit.*, pp. 200 à 204.
50. On pense notamment au cas où il dépose des cookies sur le disque dur d'un surfeur européen lors de la consultation de son site web.

Chapitre 3. Légitimité et licéité des traitements poursuivis par l'entreprise

260 **Principe**

La loi vise avant tout à créer un lieu d'équilibre entre les intérêts du responsable du traitement et ceux de la personne concernée. Son but n'est pas d'interdire à l'entreprise de traiter des données à caractère personnel.

Le principe reste la liberté de traitement, bridée par le respect du principe de finalité. Un traitement peut être poursuivi dès lors qu'il respecte les libertés individuelles de l'individu. Cette condition est dépendante du but d'utilisation des données et de la corrélation nécessaire qui doit exister entre les données et ce but d'utilisation. Nous verrons que la loi détermine largement *a priori* les hypothèses dans lesquelles la finalité du traitement peut être acceptée.

Seules certaines catégories de données – les données dites « sensibles » – obéissent à la règle inverse: interdiction de traitement sauf exception prévue par ou en vertu de la loi.

D'autre catégories de règles limitent aujourd'hui la liberté de traitement du responsable: certains transferts transfrontières de données sont interdits, de même que les décisions dites « automatisées ». Enfin, le Roi peut édicter des conditions particulières de mise en œuvre de traitements présentant des risques particuliers.

SECTION 1. LE PRINCIPE DE FINALITÉ

270 **Dispositions fondamentales: les articles 4 et 5 de la loi**

Les articles 4 et 5 de la loi posent deux principes distincts, mis en évidence par la doctrine [51].

Le premier – *principe de légitimité* – postule que le but du traitement soit déterminé, explicite et légitime [52]. L'article 5 de la loi prévoit une liste d'hypothèses dans lesquelles les finalités de traitement sont *a priori* légitimes.

Le second – *principe de conformité* – exige un lien étroit entre l'utilisation des données et la finalité légitime déclarée. Toute utilisation des données doit être compatible avec la finalité. Plus précisément, les données doivent être adéquates, pertinentes et non excessives par rapport à cette finalité.

A ces principes s'ajoutent également les règles de loyauté et de licéité inscrites à l'article 4, § 1er, 1° ainsi que l'obligation d'exactitude des informations inscrites à l'article 4, § 1er, 4°.

---

51. Voir principalement, Th. LÉONARD et Y. POULLET, 'Les libertés comme fondement de la protection des données nominatives', in F. RIGAUX, *La vie privée une liberté parmi les autres?,* Travaux de la Faculté de droit de Namur n° 17, Bruxelles, Larcier, 1992, p. 231 et s.; S. GUTWIRTH, 'De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens', *T.P.R.*, 1993, p. 1409 et s.
52. Article 4, § 1er, 2° de la loi: '*Les données à caractère personnel doivent être: (...) 2°. collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables (...)*'.

Sous-section 1. La légitimité de la finalité

280 Hypothèses de légitimité des finalités prévues à l'article 5

L'article 5 de la loi distingue six hypothèses dans lesquelles la poursuite d'un traitement est *a priori* légitime. Quatre peuvent concerner l'entreprise du secteur privé [53]. La quatrième retiendra principalement notre attention.

Le traitement peut d'abord avoir lieu « *si la personne concernée a indubitablement donné son consentement* ». Le consentement dont il s'agit doit bien évidemment répondre aux conditions contenues dans la définition légale [54].

Le traitement se justifie également *a priori* s'il est « *nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci* ». Les traitements nécessaires à l'exécution d'un service demandé ou de la livraison d'un bien acheté par la personne concernée en sont des exemples d'application.

La disposition permet aussi le traitement de données « *nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance* ». On peut citer à titre d'exemple des obligations qui s'imposent aux employeurs telles que la tenue d'une comptabilité particulière ou un registre du personnel accessible aux inspecteurs chargés du contrôle de la législation sociale, la communication de certaines données de leur personnel aux organismes de sécurité sociale, etc.

290 Hypothèse particulière de l'équilibre des droits, libertés et intérêts en présence

L'article 5, f) précise qu'un traitement peut être poursuivi si « *il est nécessaire à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée* ».

Cette hypothèse tranche avec la précision des autres cas de légitimité prévus par la loi. Elle exprime un standard, une règle ouverte: c'est au cas par cas qu'il conviendra d'opérer la balance des intérêts en présence.

Eu égard au but de la protection – le respect de la vie privée de la personne concernée par les données, et de manière générale, le respect des libertés individuelles – la loi ne peut admettre des finalités de traitement qui impliquent une violation injustifiée des droits et libertés de la personne concernée.

De manière plus précise, la loi subordonne ici la légitimité de la finalité à trois conditions cumulatives:

a. *L'existence d'un intérêt légitime poursuivi par le responsable du traitement ou le tiers auquel les données sont communiquées.* Un intérêt est légitime lorsqu'il n'est contraire à aucune loi ou règlement en vigueur. Jugé par exemple que la lutte contre la fraude à l'assurance et l'appréciation correcte du risque ainsi que la personnalisation des primes constituaient des intérêts légitimes pour des compagnies d'assurance regroupées dans une entité spécifique en vue d'échanger des informations relatives à des personnes représentant des risques particuliers [55].

---

53. On ne parle pas ici des hypothèses où le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne ou est nécessaire à l'exécution d'une mission d'intérêt public (art. 5 d) et e) de la loi).
54. Voir *supra*, n° 190.
55. Civ. Bruxelles (Prés.), 19 décembre 2000, *Bull. ass.*, 2001, p. 266 et s. et note Ch. van Oldeneel (cette décision est frappée d'appel).

b. *Le lien de nécessité entre l'existence du traitement et la réalisation de l'intérêt légitime.* Si d'autres moyens moins attentatoires aux libertés individuelles que le traitement en cause apportent au responsable un résultat analogue, il ne peut choisir la voie la plus dommageable. Jugé que ni le système du *bonus-malus*, ni celui de la segmentation de la clientèle n'énerve, pour les assureurs, la nécessité de constituer une banque de données centrale afin d'apprécier correctement le risque et de personnaliser les primes [56].

c. *La non-prépondérance d'un intérêt, d'un droit ou d'une liberté fondamentale de la personne concernée.* Même si le responsable du traitement poursuit un intérêt légitime au moyen d'un traitement qui paraît nécessaire, la finalité poursuivie ne sera considérée comme légitime que si la balance des intérêts, libertés et droits en présence penche en sa faveur.

Ont ainsi été jugées légitimes sur la base d'un équilibre des intérêts en présence, les finalités de lutte contre la fraude à l'assurance et d'appréciation correcte des primes d'une centrale de risques en matière d'assurance [57] ainsi que les finalités de promotion et de prospection commerciale en général [58]. Ont par contre été jugés illégitimes la même finalité de prospection commerciale poursuivie au départ d'une analyse des données contenues dans des virements en vue d'une opération de marketing de produits d'assurance [59] ainsi que le traitement de noms et d'adresses en vue de la confection d'un annuaire et de sa distribution gratuite à des fins de démarchages commerciales [60].

La Commission de la protection de la vie privée s'est prononcée à de nombreuses reprises sur l'application de la disposition commentée, dans un sens parfois contraire aux solutions jurisprudentielles précitées. Ainsi, par exemple, elle s'est montrée très sévère à l'égard des centrales de données, que ce soit dans le secteur de l'assurance [61] ou dans celui de l'immobilier [62]. Elle a également considéré que l'équilibre n'était pas respectée en cas de finalités de prospection commerciale impliquant des collectes de données sur internet relatives à des mineurs n'ayant pas atteint l'âge de discernement [63], d'enregistrements de communications téléphoniques dans un but de marketing

56. *Idem*.
57. Civ. Bruxelles (Prés.), 19 décembre 2000, *Bull. ass.*, 2001, p. 266 et s. et note Ch. VAN OLDENEEL (cette décision est frappée d'appel); Civ. Nivelles (Prés.), 28 octobre 2003, *Bull. ass.*, 2004, p. 49 et s. et note Ch. VAN OLDENEEL concernant la seule finalité de lutte contre la fraude.
58. Comm. Anvers (Prés.), 7 juillet 1994 et Comm. Bruxelles (Prés.), 15 septembre 1994, *Computerrecht*, 1994, p. 244 et s. et note J. DUMORTIER et Fr. ROBBEN; *D.I.T.*, 1995, p. 55 et note O. LESUISSE; pour d'autres commentaires sous ces décisions, voir *D.C.C.R.*, 1994, p. 83 et s. et note Th. LÉONARD; S. GUTWIRTH, 'De ontdekking van de privacy van de burgers als doeltreffend wapen in de strijd tussen concurrenten', note sous Comm. Bruxelles (réf.), 15 septembre 1994, *Jaarboek Handelspraktijk 1994*, Diegem, Kluwer Rechtswetenschappen, 1995, p. 361 et s.; J-P. BUYLE, L. LANNOYE, Y. POULLET, V. WILLEMS, 'Le droit de l'informatique Chronique de jurisprudence (1987-1994)', *op. cit.*, p. 236, n° 72.
59. Anvers (5e ch.), 3 mai 1999, *A.J.T.*, 1999-2000, p. 437 et s. et note C. DE VOS sur appel de la décision précitée du tribunal de commerce du 7 juillet 1994. La Cour est donc plus sévère que le tribunal sur le point de la légitimité: la décision dont appel considérait les données comme excessives eu égard à la finalité de marketing et se plaçait sur le seul terrain de la conformité des données au regard de la finalité poursuivie (*cf.* sur ce point, Th. LÉONARD, « La banque, le courtier et la vie privée: une première décision jurisprudentielle », note sous Comm. Anvers (Prés.), 7 juillet 1994, *D.C.C.R.*, 1994, p. 8 et s., n° 6).
60. Corr. Gand, 22 janvier 2000, *Computerrecht*, 2001, p. 263 et s.
61. Avis de la Commission de protection de la vie privée n° 21/2000 du 28 juin 2000 relatif au fichier RSR, http://www.privacy.fgov.
62. Avis de la Commission de protection de la vie privée n° 52/2002 du 19 décembre 2002 relatif à la constitution d'un fichier externe des locataires défaillants, http://www.privacy.fgov.
63. Avis de la Commission de la protection de la vie privée n° 38/2002 du 16 septembre 2002 relatif à la protection de la vie privée des mineurs sur l'internet, http://www.privacy.fgov.

ou d'information de la clientèle [64], de collecte d'informations relatives à la navigation et au comportement d'un internaute sur un site de commerce électronique [65], etc.

Il faut toutefois être attentif au fait que l'équilibre à analyser est dépendant des éléments spécifiques de fait et de droit qui entourent le traitement. Toute généralisation – comme l'affirmation que toute finalité de marketing est forcément légitime – est donc à proscrire.

300 Règle de compatibilité des finalités

La finalité poursuivie doit être déterminée. Cette condition formelle renvoie au principe de transparence des traitements, exprimée à divers endroits de la loi [66].

Une finalité secrète est contraire à l'article 4 de la loi. Il en découle deux conséquences importantes pour le responsable du traitement.

Une finalité doit toujours être énoncée de manière claire, complète et précise par le responsable du traitement, soit dans l'exécution de ses obligations d'information, soit dans l'exercice de son obligation de déclaration, de sorte qu'un contrôle de celle-ci soit rendue possible. Une banque a, dès lors, été condamnée car elle poursuivait une finalité de marketing de produits d'assurance alors que la finalité annoncée de son traitement précisait viser la « *prospection pour les différents services financiers* » [67].

Une finalité ne peut être détournée. Une fois annoncée, la finalité doit être respectée, c'est-à-dire que les données ne peuvent être utilisées de manière incompatible avec cette finalité. La loi précise cependant que la compatibilité doit tenir compte de tous les facteurs pertinents, « *notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables* ».

La Commission de protection de la vie privée a, dans ses avis, mis en avant à diverses reprises des exemples de finalités incompatibles avec celles annoncées par le responsable du traitement: la photo présente sur un badge d'identification ne peut être réutilisée par un employeur en vue de l'édition d'une brochure de présentation de l'entreprise [68]; des données communiquées par un acheteur pour les besoins d'une transaction ne peuvent être réutilisées et transmises par le vendeur à un tiers qui serait intéressé par le profil du client [69]; l'utilisation à des fins de prospection commerciale de données d'identification collectées en vue de la confection d'un annuaire téléphonique [70], etc.

---

64. Recommandation de la Commission de protection de la vie privée n° 01/2002 du 22 août 2002 relative à l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, http://www.privacy.fgov.
65. Avis de la Commission de la protection de la vie privée n° 34/2000 du 22 novembre 2000 relatif à la protection de la vie privée dans le cadre du commerce électronique, http://www.privacy.fgov.
66. *Cf. infra* n° 520 et s., le commentaire des obligations d'information et de déclaration des traitements automatisés.
67. Comm. Anvers (Prés.), 7 juillet 1994, *op. cit.*, *cf.* note 39. Certains commentateurs ont dès lors énoncé avec raison que '*Ainsi, la jurisprudence précise que doit faire l'objet d'une transparence chaque traitement, c'est-à-dire tout ensemble d'opérations marquées par une finalité unique telle que la personne concernée puisse raisonnablement, à la lecture de l'énoncé de cette finalité, concevoir les types d'opérations couvertes par cette finalité*' (J-P. BUYLE, L. LANNOYE, Y. POULLET, V. WILLEMS, « Le droit de l'informatique Chronique de jurisprudence (1987-1994) », *op. cit.*, p. 233, n° 65, *in fine*).
68. Avis de la Commission de la protection de la vie privée n° 2/2004 du 26 février 2004 relatif aux badges d'identification sur lesquels figurent le nom et/ou la photo du détenteur du badge, http://www.privacy.fgov.be.
69. Avis de la Commission de la protection de la vie privée n° 34/2000 du 22 novembre 2000 relatif à la protection de la vie privée dans le cadre du commerce électronique, http://www.privacy.fgov.
70. Recommandation de la Commission de la protection de la vie privée n° 1/1999 du 23 juin 1999 relative à l'utilisation des données contenues dans les annuaires téléphoniques, http://www.privacy.fgov.

Est-ce à dire que le responsable du traitement ne peut, en cours de traitement, modifier les finalités de ce dernier et, ainsi, le faire évoluer? Le cas le plus évident est celui de l'entreprise qui désire utiliser les données relatives à sa clientèle en vue de poursuivre une finalité de marketing direct alors qu'elle n'avait pas annoncé cette finalité au moment de la collecte des données. D'après nous, une telle modification des finalités doit être possible à la condition que la nouvelle finalité satisfasse à l'ensemble des conditions légales et soit considérée comme un nouveau traitement à part entière (information spécifique sur la nouvelle finalité, légitimation de celle-ci, le cas échéant, déclaration auprès de la Commission, etc.) [71]. Cette possibilité est cependant rejetée par certains qui prônent une application stricte du principe de compatibilité et n'admettent une nouvelle finalité que si elle est couverte par le consentement de la personne concernée [72].

310 Exception des traitements ultérieurs à finalités historiques, statistiques ou scientifiques

A titre d'exception à la règle de compatibilité des finalités, la loi précise en son article 4, § 1er, 2° que n'est pas réputé incompatible un traitement ultérieur à des fins historiques, statistiques ou scientifiques lorsqu'il est effectué conformément aux conditions fixées par le Roi.

Un double régime s'instaure donc concernant la poursuite de telles finalités. Si la finalité initiale annoncée est une finalité historique, statistique ou scientifique, le traitement reste soumis aux seules règles légales commentées. Si, par contre, la finalité annoncée lors de la collecte était différente et incompatible avec de telles finalités – par exemple, l'exécution d'un contrat de prestation de services – et qu'ultérieurement le responsable du traitement veut utiliser ces données en vue de réaliser, par exemple, une étude statistique de marché, il doit se conformer au régime complexe organisé par les articles 2 à 24 de l'arrêté royal.

Cette réglementation particulière ne peut être analysée dans le cadre du présent commentaire général de la loi. Nous nous permettons donc de renvoyer le lecteur à l'arrêté royal précité ainsi qu'aux commentaires particuliers auxquels il a donné lieu [73]. Ces dispositions sont toutefois capitales pour certaines entreprises privées ayant par exemple pour objet la recherche médicale ou la production de statistiques privées (études de marché, etc.).

Retenons seulement ici que le principe de base est qu'il incombe au responsable du traitement de ne travailler qu'avec des données anonymes. Si cela s'avère impossible, il doit alors coder les données et se soumettre aux règles particulières propres aux traitements de telles données. Si un tel codage est impossible, il doit se soumettre au régime spécifique au traitement de données non codées. Les conditions de traitement sont à chaque étape de plus en plus strictes: de l'absence de protection pour les données anonymes à un régime de consentement préalable pour les données non codées.

---

71. Th. Léonard et Y. Poullet, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, p. 385, n° 30. Dans le même sens, D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 118 et s., nos 154 à 156.
72. Voir par exemple J. Dumortier, 'De nieuwe wetgeving over de verwerking van persoonsgegevens', in *Recente ontwikkelingen in informatica- en telecommunicatierecht*, Bruges, Die Keure, 1999, p. 86. Dans le même sens, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 29.
73. Voir par exemple, I. Anné, 'De verwerking van persoonsgegevens voor wetenschappelijk onderzoek', *Computerrecht*, 2000, pp. 288 à 296; D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, pp. 101 à 110; C. de Terwangne et S. Louveaux, 'La protection de la vie privée face au traitement de données à caractère personnel: le nouvel arrêté royal', *J.T.*, 2001, pp. 465 à 469.

Sous-section 2. La conformité des données

320 Caractère adéquat, pertinent et non excessif des données

Une finalité déterminée, explicite et légitime n'autorise pas d'elle-même l'utilisation de n'importe quelle donnée.

Le principe de conformité implique que les données utilisées soient adéquates, pertinentes et non excessives par rapport à la finalité déterminée et légitime. On retrouve ici explicitement une règle de proportionnalité.

L'adéquation et la pertinence de la donnée visent une liaison nécessaire et suffisante de l'information par rapport au but poursuivi par le traitement. Si un particulier désire s'abonner à une newsletter sur internet, son adresse e-mail constitue une donnée adéquate et pertinente au regard de la finalité d'inscription. D'autres informations comme son nom, son adresse et ses centres d'intérêts seraient par contre inadéquates et non pertinentes au vu de cette seule finalité [74].

Le caractère non excessif de la donnée exige que même si son utilisation s'avère nécessaire au vu de la finalité poursuivie, elle ne soit pas retenue si elle présente un risque d'atteinte disproportionnée par rapport aux intérêts individuels de la personne concernée. Il a ainsi été jugé, de manière sans doute critiquable [75], que les données relatives aux nom et adresse du destinataire d'un virement, aux raisons du paiement et au montant ne pouvaient sans violer le principe de conformité être traitées par une banque en vue d'une finalité de marketing [76]. Une autre décision a considéré que le traitement systématique d'informations sur les bénéficiaires de virements était excessif par rapport aux finalités de gestion de compte et de marketing [77]. La Commission a aussi considéré que si un badge d'identification était utilisé dans une grande entreprise en vue de contrôler les déplacements du personnel, les mentions des nom et prénom de la personne étaient disproportionnées, au contraire de sa photo et d'un numéro de référence unique [78].

330 Durée de conservation limitée des données – Droit à l'oubli

Les données ne peuvent être conservées indéfiniment par le responsable du traitement. Ce principe est à ce point essentiel pour la personne concernée par les données qu'il a débouché sur la reconnaissance d'un droit spécifique: le droit à l'oubli.

---

74. Avis de la Commission de la protection de la vie privée n° 34/2000 du 22 novembre 2000 relatif à la protection de la vie privée dans le cadre du commerce électronique, http://privacy.fgov.be. Par contre, comme le relève la Commission, ces données pourraient s'avérer adéquates et pertinentes au regard d'une finalité distincte comme le profilage des abonnés, finalité qui devrait alors être annoncée comme telle par le responsable du site internet.
75. J-P. Buyle, L. Lannoye, Y. Poullet, V. Willems, 'Le droit de l'informatique Chronique de jurisprudence (1987-1994)', *op. cit.*, p.236, n° 72 et réf. citées; Th. Léonard, 'La banque, le courtier et la vie privée: une première décision jurisprudentielle', note sous Comm. Anvers (Prés.), 7 juillet 1994, *D.C.C.R.*, 1994, p. 77 et s., spéc. p. 88.
76. Comm. Anvers (Prés.), 7 juillet 1994, *op. cit*.
77. Comm. Bruxelles (Prés.), 15 septembre 1994, *op. cit.*
78. Avis de la Commission de la protection de la vie privée n° 2/2004 du 26 février 2004 relatif aux badges d'identification sur lesquels figurent le nom et/ou la photo du détenteur du badge, http://www.privacy.fgov.be.

L'article 4, 5° de la loi précise que les données doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement* ». La non-utilisation des données en vue de la finalité poursuivie implique donc leur effacement. La durée de conservation d'une donnée doit toujours être justifiée au regard de la finalité poursuivie.

Faisant application de ce principe, le Président du Tribunal de première instance de Bruxelles a ainsi décidé que la conservation durant deux ans de données relatives à des débiteurs défaillants par la Banque Nationale de Belgique n'était pas excessive eu égard à la finalité poursuivie par ce type de traitement [79].

SOUS-SECTION 3. LES RÈGLES DE LOYAUTÉ, DE LICÉITÉ ET D'EXACTITUDE

340 Règles de licéité et de loyauté

L'article 4, § 1er, 1° de la loi dispose que les données doivent être traitées loyalement et licitement.

Pour être *licite*, un traitement de données doit respecter l'ensemble des prescrits légaux et réglementaires applicables. Outre le prescrit de la loi sur la protection des données, d'autres dispositions peuvent conditionner le traitement de certaines données. Ainsi en est-il, par exemple, du traitement de l'adresse e-mail en vue d'une finalité de publicité. L'article 14 de la loi du 11 mars 2003 – loi dite e-commerce – interdit en effet l'utilisation du courrier électronique à des fins de publicité sans le consentement préalable, libre, spécifique et informé du destinataire du message et impose des obligations particulières, notamment une information spécifique au bénéfice au destinataire de la publicité [80]. Le traitement de l'adresse e-mail dans une finalité de publicité doit donc, pour être licite, se conformer à ces dispositions dans la limite de son champ d'application [81].

La *loyauté* du traitement évoque, principalement, la transparence des actions. Cette transparence doit être assurée dès la collecte, notamment par le biais de l'obligation d'informer la personne concernée. Cette dernière doit savoir quel est le but d'utilisation des données, entre quelles mains elles se trouvent, à quelles fins elles sont communiquées, etc. [82]. La loyauté peut également proscrire certaines collectes d'information considérées comme inacceptables au vu, par exemple, des circonstances dans lesquelles elles ont lieu: la Commission de protection de la vie privée considère ainsi qu'apparaît comme déloyale la collecte auprès d'un mineur d'âge de données concernant son entourage, telles que les centres d'intérêts ou les habitudes de consommation des membres de sa famille [83].

---

79. Civ. Bruxelles (Prés.), 13 septembre 1995, *D.C.C.R.*, 1996, p.57 et s. et note Th. LÉONARD.
80. Sauf exception prévue par l'arrêté royal du 4 avril 2003 visant à réglementer l'envoi de publicité par courrier électronique.
81. On pense également à la convention collective de travail n° 68 conclue le 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail et à la convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électronique en réseau.
82. Voir *supra* n° 530 et s., le contenu de l'obligation d'information.
83. Avis de la Commission de la protection de la vie privée n° 38/2002 du 16 septembre 2002 relatif à la protection de la vie privée des mineurs sur l'Internet, http://www.privacy.fgov.be.

350 **Obligation d'exactitude des données**

L'article 4, § 1er, 4° de la loi énonce que les données traitées doivent être exactes et, si nécessaire, mises à jour. Il précise que « *toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement soient effacées ou rectifiées* ».

Le prescrit de cette disposition incite à penser qu'il s'agit d'une obligation de diligence qui est mise à charge du responsable du traitement. Le critère à prendre en compte serait donc celui du responsable normalement prudent et diligent [84]. Le doute est cependant permis si l'on se réfère à l'article 15*bis* de la loi qui pourrait établir un régime particulier de responsabilité civile [85].

SECTION 2. LE TRAITEMENT DES DONNÉES SENSIBLES

360 **Généralités**

La loi distingue trois types de données « sensibles »: les données sensibles au sens strict, les données relatives à la santé, et les données judiciaires. Les traitements de ces données sont, en règle, interdits sauf exception établie par la loi elle-même. La loi charge en outre le Roi de prévoir quelles sont les conditions particulières auxquelles doivent alors satisfaire les traitements permis de telles données. Ces conditions sont prévues aux articles 25 à 27 de l'arrêté royal.

Nous analyserons d'abord la portée de l'interdiction et des exceptions pour chacune des catégories de données sensibles. Nous analyserons ensuite les conditions particulières de traitement qui s'appliquent à ces différentes exceptions.

SOUS-SECTION 1. LE RÉGIME DES DONNÉES SENSIBLES AU SENS STRICT

370 **Donnée sensible: notion**

Les données sensibles au sens strict sont énumérées à l'article 6 de la loi. Il s'agit des données « *qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que (les) données relatives à la vie sexuelle* ».

La notion de donnée sensible, modifiée par la loi du 11 décembre 1998, s'élargit au regard de l'ancien texte. En effet, mises à part les données relatives à la vie sexuelle, une donnée est sensible si elle « révèle » une des informations visées par le nouveau texte. Comme l'explique l'exposé des motifs, les données ne doivent pas, par exemple, se rapporter directement aux origines raciales ou ethniques pour tomber sous le champ de la disposition mais il suffit que la race ou l'origine ethnique puisse être déduites des données [86].

---

84. Voir en ce sens, D. DE BOT, *Verwerking van persoonsgegevens*, *op. cit.*, p. 127, n° 167; Th. LÉONARD et Y. POULLET, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, p. 385, n° 31.
85. *Cf. supra*, n° 900 concernant le contenu de cette disposition.
86. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, pp. 33 et 34.

Les excès de l'application stricte de cette disposition ont été soulignés [87]. Ainsi, par exemple, un virement contenant la mention d'un syndicat comme bénéficiaire et la communication « cotisation 2004 » révèlerait l'appartenance syndicale et le traitement de ces données, nécessaire à l'opération de paiement, serait donc interdit *a priori*. L'exposé des motifs paraît se rendre compte de la difficulté lorsqu'il en appelle à une application raisonnable de la disposition [88].

380 Exceptions légales au régime d'interdiction de traitement des données sensibles

L'article 6, § 2 de la loi lève l'interdiction de traitement des données sensibles au sens strict dans les hypothèses qu'il détermine. Seules les exceptions intéressant normalement l'entreprise sont commentées ci-dessous.

390 Consentement écrit de la personne concernée

L'article 6, § 2, a) de la loi énonce que les données sensibles au sens strict peuvent faire l'objet d'un traitement lorsque « *la personne concernée a donné son consentement par écrit à un tel traitement pour autant que ce consentement puisse à tout moment être retiré par celle-ci* ». Le consentement doit bien évidement répondre aux conditions de sa définition légale [89].

Il en découle que la personne concernée doit être précisément informée de la ou des finalité(s) d'utilisation des données sensibles qui vont être traitées. La finalité trace donc les limites de la portée du consentement. Ce consentement, comme la finalité sur laquelle il porte, ne peut être ni général, ni ambigu.

La personne peut à tout moment retirer son consentement. Il s'agit, alors, d'un véritable droit d'opposition à rebours.

400 Traitement nécessaire à l'application du droit du travail

L'interdiction tombe également lorsque le traitement poursuivi est nécessaire « *afin d'exécuter les obligations et droits spécifiques du responsable du traitement en matière de droit du travail* » [90].

Cette exception doit être interprétée de manière stricte. Seuls les traitements imposés par une règle du droit du travail sont visés. On a pensé ici aux traitements poursuivis en exécution de la réglementation de la médecine du travail, des congés politiques et syndicaux, des empêchements (communion solennelle, ordination, etc.), des suspensions du contrat de travail pour cause de grossesse ou d'allaitement, etc.

Il découle de cette interprétation que tout enregistrement de données sensibles dans la relation entre l'employeur et son personnel n'est pas automatiquement permis par cette exception.

---

87. Th. Léonard et Y. Poullet, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, p. 386, n° 6.
88. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 34: '*cette disposition doit naturellement être appréciée de manière raisonnable au sens où les informations sensibles doivent pouvoir être déduites des données avec certitude ou avec une probabilité quasi certaine. On ne peut conclure par exemple à la conviction religieuse d'une personne avec certitude ou avec quasi certitude sur la base du seul fait qu'elle commande un exemplaire de la Bible à une société de vente par correspondance*'. Dans le même sens, sauf modification du texte légal, D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 141, n° 184.
89. *Cf. supra*, n° 190.
90. Article 6, § 2, b) de la loi.

410 **Exceptions diverses**

D'autres exceptions pourront également intéresser l'entreprise. On peut ainsi citer les hypothèses suivantes:

a. Le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement [91].
b. Le traitement est effectué, dans le cadre de leurs activités légitimes, par une fondation, une association, ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées [92].
c. Le traitement porte sur des données manifestement rendues publiques par la personne concernée [93].
d. Le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice [94].
e. Le traitement est nécessaire à des recherches scientifiques et est effectué aux conditions fixées par arrêté royal [95].
f. Le traitement est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée soit à un parent ou de la gestion des services de santé agissant dans l'intérêt de la personne concernée et que le traitement est effectué sous la surveillance d'un professionnel des soins de santé. Dans ce cas, le professionnel des soins de santé et ses préposés ou mandataires sont soumis au secret [96].

Les autres exceptions prévues par la loi n'intéressent normalement pas l'entreprise.

Sous-section 2. Les données relatives à la santé

420 **Donnée relative à la santé: notion**

Le nouvel article 7 de la loi ne définit plus ce qu'il faut entendre par les données relatives à la santé [97].

L'exposé des motifs invite à reconnaître une portée plus étroite à la donnée «*relative à la santé*» [98]. Alors que les données qui «*révèlent*» une information

91. Article 6, § 2, c) de la loi.
92. Article 6, § 2, d) de la loi.
93. Article 6, § 2, e) de la loi
94. Article 6, § 2, f) de la loi.
95. Article 6, § 2, g) de la loi. *Cf.* les articles 14 et 16 de l'arrêté royal.
96. Article 6, § 2, j) *in fine* de la loi.
97. Précédemment, l'ancienne disposition, modifiée par la loi du 11 décembre 1998, entendait par 'données médicales' 'toutes données à caractère personnel dont on peut déduire une information sur l'état antérieur, actuel ou futur de la santé physique ou psychique, à l'exception des données purement administratives ou comptables relatives aux traitements et aux soins médicaux'.
98. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 34; voir cependant à la p. 38, la déclaration selon laquelle les données relatives à la santé seraient une catégorie de données plus large que les données médicales...

sensible se rapportent à toute information sensible « *déduite* » de la donnée – comme visé sous l'ancien texte dans la définition de la donnée médicale – celles qui sont seulement « *relatives* » à la santé doivent « *se rapporter* » à ces informations. Le Ministre en conclut que « *des données qui révèlent seulement l'état de santé ou la vie sexuelle d'un individu, mais qui ne se rapportent pas à sa santé ou à sa vie sexuelle, ne tombent pas sous le régime – plus strict – de l'article 8 de la directive* ». On peut penser ici à une photographie « *révélant* » un handicap. On a déjà souligné le manque de clarté de cette distinction.

430 Exceptions légales au régime d'interdiction de traitement des données relatives à la santé

Les exceptions au régime d'interdiction sont, pour la plupart, identiques à celles déjà relevées concernant les données sensibles au sens strict.

On retrouve donc ici le consentement écrit de la personne concernée [99], le traitement nécessaire à l'exécution d'obligations et droits issus du droit du travail [100], le traitement nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi en vue de l'application de la sécurité sociale [101], celui nécessaire à la défense d'intérêts vitaux de la personne concernée ou d'une autre personne si la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement [102], le traitement portant sur des données manifestement rendues publiques par la personne concernée [103], le traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice [104], le traitement nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée soit à un parent ou de la gestion des services de santé agissant dans l'intérêt de la personne concernée [105] et le traitement nécessaire à la recherche scientifique [106].

En outre, ne sont pas soumis à l'interdiction de traitement ceux nécessaires à la promotion et à la protection de la santé publique y compris le dépistage [107] et ceux nécessaires pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée [108].

440 Conditions légales du régime d'exception de traitement des données relatives à la santé

Ces exceptions ne sont admises que si les données relatives à la santé sont traitées sous la responsabilité d'un professionnel des soins de santé, sauf en cas de consentement de la personne concernée ou de nécessité pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée.

99. Article 7, § 2, a) de la loi.
100. Article 7, § 2, b) de la loi.
101. Article 7, § 2, c) de la loi.
102. Article 7, § 2, f) de la loi.
103. Article 7, § 2, h) de la loi.
104. Article 7, § 2, i) de la loi.
105. Article 7, § 2, j) de la loi.
106. Article 7, § 2, k) de la loi et articles 14 et 16 de l'arrêté royal.
107. Article 7, § 2, d) de la loi.
108. Article 7, § 2, g) de la loi.

On peut cependant se demander ce qu'il faut entendre par la notion de « professionnel des soins de santé » [109]. Ces termes correspondraient « à un concept vaste qui fait référence à l'ensemble des personnes qui prestent des soins de santé à l'égard d'autres personnes dans l'exercice de leur profession » [110]. Mais l'exposé vise également les personnes travaillant pour le compte de professionnels des soins de santé.

L'alinéa 3 du § 4 de la disposition commentée prévoit que « *le professionnel des soins de santé et ses préposés ou mandataires sont soumis au secret* ». L'article 39, 3° érigeant la violation de l'article 7 par le responsable du traitement, ses préposés ou mandataires, l'exposé des motifs y voit une obligation de secret sanctionnée pénalement. Les personnes intervenant dans le traitement des données relatives à la santé sont donc tenues à une sanction pénale distincte de l'article 458 du Code pénal [111].

En outre, en vertu du § 5 de l'article 7, les données relatives à la santé ne peuvent normalement être collectées qu'auprès de la personne concernée. Elle ne peuvent être collectées auprès d'autres sources que si la collecte est conforme aux conditions prescrites par le Roi, est effectuée sous la responsabilité du professionnel des soins de santé, et est nécessaire à la finalité poursuivie.

Sous-section 3. Les données judiciaires

450 Donnée judiciaire: notion

Les données dites « judiciaires » reçoivent une définition particulièrement large. Il s'agit « *des données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté* ».

Cette définition élargit celle présente dans la directive. Cette dernière ne visait ni les données relatives aux suspicions et aux poursuites ni celles relatives, de manière générale, aux « *litiges* » soumis aux cours et tribunaux. Dorénavant en droit belge, les banques ou les grands magasins ne pourront plus traiter des données relatives à des suspicions de fraudes pénales.

460 Exceptions légales au régime d'interdiction de traitement des données judiciaires

Les exceptions au principe d'interdiction, prévues par l'article 8, § 2 de la loi, sont assez limitées. L'interdiction est levée si le traitement est effectué:

a. sous le contrôle d'une autorité publique ou d'un officier ministériel au sens du Code judiciaire, lorsque le traitement est nécessaire à l'exercice de leurs tâches;
b. par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance;
c. par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige. La Commission de la protection de la vie privée a, sur cette base, considéré que l'IFPI et la Sabam pouvaient traiter des données relatives aux internautes qui téléchargent

109. Le Conseil d'Etat critique amplement l'utilisation de ce terme trop vague et ne se référant à aucun concept légal défini antérieurement (Avis du Conseil d'Etat, 2 février 1998, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 220).
110. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 39.
111. Sans préjudice de l'application de cette disposition pour les professionnels des soins de santé qu'elle vise.

des fichiers musicaux en infraction aux règles de protection du droit d'auteur mais uniquement dans le cadre d'un contentieux précis ou d'une phase préparatoire à un tel contentieux, et dans la mesure où elles représentent en justice leurs membres, maisons de disques ou artistes. Mais en aucune façon, l'exception ne permettrait à ces organismes de rechercher systématiquement et de façon proactive des données à caractère personnel sur Internet dans le but de déceler des infractions au droit d'auteur [112];

d. par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige;
e. pour les nécessités de la recherche scientifique, dans le respect des conditions fixées par le Roi.

470 Conditions communes de traitement des données sensibles prévues par arrêté royal

Même si le responsable du traitement bénéficie d'une exception au régime d'interdiction de traitement des données sensibles, il doit encore respecter les conditions particulières de tels traitements, prévues par l'arrêté royal.

Certaines sont communes aux trois catégories de données sensibles [113].

Le responsable – ou le sous-traitant – doit ainsi désigner les catégories de personnes ayant accès aux données avec une description précise de leur fonction par rapport au traitement en cause. La liste de ces catégories de personnes doit être tenue à la disposition de la Commission de la protection de la vie privée. En se référant à des catégories de personnes, le Roi n'impose pas de désigner nommément les personnes ayant accès aux données mais bien les profils ou fonctions des personnes pouvant avoir accès aux données (p. ex. les médecins et docteurs d'une clinique).

En outre, le responsable doit veiller à ce que les personnes ainsi désignées soient tenues par une obligation légale, statutaire ou contractuelle de respect du caractère confidentiel des données visées. Enfin, le responsable doit indiquer la base légale ou réglementaire qui lui reconnaît de lever l'interdiction de traitement tant dans l'information donnée à la personne concernée que dans la déclaration qu'il devra, le cas échéant, déposer auprès de la Commission de la protection de la vie privée.

D'autres conditions de traitement ne visent que les seuls traitements de données sensibles au sens strict et de données relatives à la santé [114].

Si l'interdiction de traitement de ces données est levée sur la base de l'exception du consentement, le responsable doit informer préalablement la personne des motifs du traitement de ces données et lui communiquer la liste des catégories de personnes y ayant accès.

Dans la même hypothèse, le traitement reste interdit lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis de lui, l'empêchant de refuser librement son consentement. Cette dernière interdiction est cependant levée si le traitement vise l'octroi d'un avantage à la personne concernée. Cette disposition a été justement critiquée. Outre qu'elle apparaît comme particulièrement floue, elle revient à admettre comme valable un consentement qui ne peut être reconnu comme

112. Avis de la Commission de la protection de la vie privée n° 44/2001 du 12 novembre 2001 concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications, http://www.privacy.fgov.be.
113. Article 26 de l'arrêté royal.
114. Articles 26 et 27 de l'arrêté royal.

libre dès lors qu'un avantage, aussi minime soit-il, est reconnu à la personne concernée [115].

SECTION 3. LES TRANSFERTS TRANSFRONTIÈRES DE DONNÉES

480 Principe d'interdiction des transferts de données vers des pays tiers

Le premier alinéa de l'article 21 de la loi énonce un principe: le transfert de données faisant l'objet d'un traitement après ce transfert vers un pays non membre de la Communauté européenne n'est autorisé que si le pays destinataire des données assure un niveau de protection adéquat et, ajoute la loi, moyennant le respect des autres dispositions de la présente loi et de ses arrêtés d'exécution.

L'article 21 précise en son alinéa 2 les critères d'appréciation du caractère adéquat: « *Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données. Il est notamment tenu compte de la nature finale, des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées* »

Il revient d'abord au responsable du traitement d'apprécier le caractère adéquat de la protection du destinataire [116]. Il s'aidera utilement des travaux du Groupe dit de l'article 29 de la Directive [117] qui a établi une méthodologie d'analyse des flux et a fixé les critères du caractère adéquat de la protection [118]. La Commission européenne peut du reste décider qu'un pays tiers offre un niveau de protection adéquat en raison de sa législation interne ou des engagements pris au niveau international [119].

Le Roi détermine « *pour quelles catégories de traitements et dans quelles circonstances, la transmission* » n'est pas autorisée. Cette solution de la « liste noire » est illusoire dans la mesure où l'on sait que la décision d'inscrire un pays dans la liste noire est bien trop délicate politiquement. L'utilisation par le Roi des prérogatives qui lui sont confiées par l'article 21 risque d'être exceptionnelle et de n'être jamais que le suivi d'une décision européenne.

---

115. C. DE TERWANGNE et S. LOUVEAUX, 'La protection de la vie privée face au traitement de données à caractère personnel: le nouvel arrêté royal', *op. cit.*, p. 460.
116. Pour des analyses plus précises de ce régime, voir par exemple, D. DE BOT, *Verwerking van persoonsgegevens*, *op. cit.*, p. 299 et s.; B. HAVELANGE, A.-Chr. LACOSTE, 'Les flux transfrontaliers de données à caractère personnel en droit européen', *J.T. Eur.*, 2001, p. 241 et s.
117. Document de travail adopté par le Groupe le 24 juillet 1998: 'Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données', *cf.* http://europa.eu.int/comm/internal_market/privacy. Ce document reprend les conclusions de l'étude: Y. POULLET et B. HAVELANGE, *Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel*, Janvier 1997, Annexe au rapport annuel 1998 (XV D/5047/98) du groupe de travail établi par l'article 29 de la directive 95/46/CE, Office des publications européennes, ISBN 92-828-4305-X.
118. Le document analyse également l'interprétation à donner aux exceptions prévues par l'article 26 de la directive.
119. L'effet d'une telle décision est alors que les données à caractère personnel peuvent être transférées des 25 Etats membres de l'UE et des trois Etats membres de l'EEE (Norvège, Liechtenstein et Islande) vers un pays tiers sans nécessité d'obtenir des garanties supplémentaires. Ce caractère adéquat a été notamment retenu pour la Suisse, le Canada, l'Argentine, Guernesey, l'Ile de Man, les principes de la 'sphère de sécurité' publiés par le Ministère du Commerce des Etats-Unis d'Amérique et les données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des Etats-Unis. Pour plus d'informations, *cf.* http://europa.eu.int/comm/internal_market/privacy.

Il résulte donc un triple régime en cas de transferts de données hors du territoire belge. Soit le pays destinataire est un pays européen, et le régime normal d'application territorial de la loi s'applique. Ce transfert est normalement autorisé puisque le pays destinataire présente par définition – sa loi est prise en application de la même directive européenne – un niveau de protection adéquat. Soit le destinataire est établi hors de l'Union européenne et alors il convient de vérifier s'il n'y a pas lieu de faire une application extraterritoriale de la loi en application de ses critères de rattachement [120]. Si la réponse est négative, il convient d'appliquer le régime des articles 21 et 22 de la loi.

490 **Exceptions au principe d'interdiction des transferts vers des pays tiers**

L'article 22 prévoit conformément à la directive un régime d'exceptions à l'interdiction énoncée par l'article 21 de la loi. L'article 22, § 1er vise des cas particuliers qui tiennent compte du contexte dans lequel s'inscrit le flux. Nous citerons celles susceptibles d'être utiles à une entreprise du secteur privé: la personne concernée a indubitablement donné son consentement, le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou des mesures préalables à la conclusion de ce contrat, prises à la demande de la personne concernée, le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers. Ces exceptions doivent être interprétées restrictivement.

Le § 2 du même article exige qu'à défaut de protection adéquate offerte par le pays tiers, celle-ci soit offerte par le mécanisme de « garanties suffisantes », notamment contractuelles. Ainsi, si une entreprise multinationale désire transférer les données relatives à son personnel, sans consentement de celui-ci, dans un pays n'offrant pas de protection adéquate, il lui revient par des mécanismes variés tantôt de sécurité technique, tantôt organisationnels (nomination d'un détaché chargé de veiller au respect dans le pays du destinataire des normes de protection des données), tantôt enfin par des clauses contractuelles à objet varié (reconnaissance d'un droit d'accès et de rectification, limitation des finalités d'utilisation, ...), de procurer des « *garanties suffisantes quant au respect effectif des principes de la protection des données* ».

L'article 22, § 2 laisse au Roi le soin d'autoriser de tels transferts. Le responsable s'adressera au Ministère de la Justice qui, après avis de la Commission de la protection de la vie privée, se prononcera par voie d'arrêté [121].

Il convient de noter que la Commission européenne peut décider que certaines clauses contractuelles types offrent des garanties suffisantes. Elle a ainsi adopté des clauses contractuelles types tant à destination de responsables de traitement établis en dehors de l'Union que de sous-traitants établis dans de tels pays qui ne présentent pas des protection adéquates [122]. Si le responsable établi en Belgique utilise ces clauses,

120. *Cf. supra*, n° 250.

121. Pour un exemple, voir Avis de la Commission de la protection de la vie privée n° 04/2004 du 15 mars 2004 visant à légitimer un transfert de données à caractère personnel vers des pays non membres de la Communauté européenne, http://www.privacy.fgov.be.

122. Décision de la Commission 2001/497/CE du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, *J.O.C.E.*, n° L 181/19, 4 juillet 2001, pp. 19 à 31 et Décision de la Commission 2002/16/CE du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers, *J.O.C.E.*, n° L 006, 10 janvier 2002, pp. 52 à 62. Ces clauses sont accessibles en ligne à l'adresse http://europa.eu.int/comm/internal_market/privacy/modelcontracts_fr.htm.

les données peuvent en principe être transmises vers un pays qui n'assure pas un niveau adéquat de protection des données et ainsi lever l'interdiction de principe.

SECTION 4. LES DÉCISIONS AUTOMATISÉES

500 Interdiction de principe des décisions automatisées et exceptions légales

L'article 12*bis* de la loi énonce que « *une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destinées à évaluer certains aspects de la personnalité* ». On vise principalement par là les systèmes automatisés évaluant le rendement professionnel, le crédit, la fiabilité et le comportement de la personne. Le but est d'éviter que, sans aucune intervention humaine, des décisions soient prises directement sur la base d'un résultat fourni de manière automatisée [123].

L'interdiction fait l'objet de deux larges exceptions. Elle est levée lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Le texte légal précise que ce contrat ou cette disposition doivent contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il doit au moins lui être permis de faire valoir utilement son point de vue.

SECTION 5. LES TRAITEMENTS PRÉSENTANT DES RISQUES PARTICULIERS

510 Le régime de certains traitements particuliers prévu par l'article 17*bis* de la loi

L'article 17*bis* de la loi charge le Roi, après avis de la Commission de la protection de la vie privée, de déterminer des catégories de traitements qui présentent des risques particuliers « *au regard des droits et libertés des personnes concernées* » et de fixer dans ces hypothèses des conditions particulières garantissant ces droits et libertés.

Le texte légal cite explicitement comme exemple de garantie la désignation par le responsable du traitement d'un préposé à la protection des données chargé d'assurer, de manière indépendante, l'application de la loi et de son arrêté. Le Roi est chargé, toujours après avis de la Commission, de déterminer le statut d'un tel préposé. A ce jour, cette disposition n'a pas reçu d'application en l'absence d'arrêté royal ayant cet objet.

123. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 17.

Chapitre 4. Obligations de l'entreprise

520 **Généralités**

Le responsable du traitement est soumis à une série d'obligations en vue d'assurer la transparence des traitements poursuivis et la possibilité d'un contrôle effectif de ceux-ci tant par la personne concernée par les données que par la Commission de la protection de la vie privée ou par le juge.

Il doit ainsi informer la personne concernée des caractéristiques de ses traitements afin de lui permettre d'accéder aux données, voire d'en demander la rectification ou de s'y opposer.

Le cas échéant, le responsable du traitement devra déclarer ses traitements automatisés auprès de la Commission de la protection de la vie privée.

Enfin, le responsable et le soustraitant sont soumis à des obligations de sécurité et de confidentialité.

SECTION 1. L'OBLIGATION D'INFORMATION

530 **Objet de l'obligation d'information**

La loi conserve un double régime d'information de la personne concernée selon que le responsable du traitement a « *obtenu* » [124] les données auprès de la personne concernée (art. 9, § 1er de la loi) ou auprès d'une autre personne (art. 9, § 2).

Dans les deux situations, la loi impose une information minimale de la personne concernée: l'information sur le nom et l'adresse du responsable du traitement et les finalités du traitement. Elle ajoute une information complémentaire lorsque la finalité de direct marketing est « *envisagée* » par le responsable du traitement: la personne concernée doit être informée de son droit d'opposition à un tel traitement [125].

La loi oblige aussi le responsable du traitement à fournir des informations « *supplémentaires* » suivant le critère qu'elle détermine. Ces informations visent, notamment, les catégories de données, les catégories de destinataires, le caractère obligatoire ou non de la réponse et l'existence d'un droit d'accès et de rectification. Ces informations supplémentaires ne doivent pas être communiquées à la personne si, au regard des circonstances de l'obtention des données, elles ne sont pas nécessaires pour assurer un « *traitement loyal des données* ».

D'autres informations « *supplémentaires* » devront donc être transmises, le cas échéant, en fonction de l'application de ce critère de loyauté. Ainsi, si le traitement se déroule en partie à l'étranger, ce fait doit être révélé, au vu des risques accrus que le transfert de données implique pour la personne concernée.

Le Roi peut toujours imposer une information supplémentaire en fonction du caractère spécifique du traitement.

Dans les deux hypothèses d'information, l'obligation est levée si la personne a déjà reçu l'information en cause antérieurement.

---

124. Le mot '*collecte*' implique une démarche active du responsable du traitement alors que l'expression '*obtenir des données*' vise également la situation dans laquelle la personne concernée communique spontanément les données à caractère personnel (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, no 1566/1, p. 44).
125. Sur le contenu de ce droit d'opposition, *cf. infra* no 640 et s.

540 Procédure d'information

Aucune procédure particulière d'information n'est spécifiée par la loi. Celle-ci peut donc être écrite ou orale, transmise par voie électronique, collective ou particulière.

Des procédures collectives supplémentaires s'imposeront souvent pour les traitements relatifs au personnel de l'entreprise, le cas échéant dans le respect de règles particulières prévues par le droit du travail. Citons à titre d'exemple, les procédures spécifiques d'information prévues par la convention collective de travail n° 68 conclue le 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail et par la convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électronique en réseau. Il convient d'être attentif au fait que ces textes, ainsi que d'autres [126], peuvent venir modaliser le régime d'information prévu par la loi. Il convient donc de vérifier tous les textes applicables avant d'organiser la transmission des informations à la personne concernée.

Le responsable du traitement pourra s'inspirer utilement des procédures préconisées par la Commission à l'égard de certains traitements particuliers. On pense par exemple à l'information à communiquer dans le cadre des traitements poursuivis dans une relation d'e-commerce [127].

Généralement, l'information lors de la collecte s'effectue par l'insertion d'une clause-type sur un questionnaire, un coupon ou un courrier transmis à la personne concernée. La principale difficulté rencontrée consiste souvent à éviter au maximum que l'information transmise ne prenne une place trop importante sur le document.

Dès lors qu'un lien contractuel lie le responsable du traitement à la personne concernée, une insertion de l'information dans le contrat ou les conditions générales est souvent la solution la plus simple. Il ne faut toutefois pas oublier que l'information est censée précéder la conclusion du contrat.

Le mode d'information ne doit pas consister forcément en un écrit. Il peut être oral, par exemple lors d'une collecte d'informations par téléphone. L'important est alors de se constituer une preuve de la réalité de l'information. Cette preuve pourra être tirée de diverses présomptions comme par exemple une note interne aux employés chargés du démarchage, où il est précisé les informations qui doivent obligatoirement être transmises à la personne concernée, ou une confirmation lors d'un envoi éventuel de documents, etc.

550 Spécificités de l'information en cas d'obtention des données auprès de la personne concernée

Il convient de noter que ni la loi ni l'arrêté d'exécution ne prévoient d'exception à l'obligation d'information lorsque les données sont obtenues par le responsable directement auprès de la personne concernée.

C'est pourquoi il convient d'insister sur la portée extrêmement large de cette obligation. Quels que soient la qualité du responsable, le type de relation entretenue avec la personne, la nature des données, etc., le responsable doit informer la personne des éléments prévus par la loi.

---

126. Par exemple, celle imposée en cas de finalités ultérieures scientifiques, statistiques et historiques (*cf. supra*, n° 310) ou de finalité de publicité de courriers électroniques (*cf. supra*, n° 340).
127. Avis n° 34/2000 du 22 novembre 2000 relatif à la protection de la vie privée dans le cadre du commerce électronique, http://www.privacy.fgov.be.

L'information doit parvenir à la personne concernée « *au plus tard au moment où ces données sont obtenues* ». Cette précision a été insérée à la demande de la Commission qui, considérant que normalement l'information devait être effectuée au moment de la collecte des données, insistait sur le fait que la personne devait avoir la possibilité de refuser la transmission des données sur la base des informations transmises préalablement par le responsable [128].

560 **Spécificités de l'information en cas d'obtention des données auprès d'une personne autre que la personne concernée**

L'information doit ici être transmise dès l'enregistrement des données, et si une communication à un tiers est envisagée, au plus tard lors de la première communication à ce tiers.

Si la communication ou l'utilisation des données a lieu à des fins de marketing direct, la personne concernée doit être avertie avant la communication au tiers ou l'utilisation pour le tiers afin de pouvoir exercer en temps utile son droit d'opposition.

Autre particularité: la loi a prévu deux exceptions à l'obligation d'information lorsque les données ne sont pas obtenues de la personne concernée.

La première exception vise les cas où « *l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés* ». Le prescrit légal vise, en particulier, les traitements à finalité statistique, de recherche historique ou scientifique et ceux poursuivis pour le dépistage motivé par la protection et la promotion de la santé publique. Les contours de l'impossibilité d'information et du caractère disproportionné des efforts demandés pas l'obligation d'information au responsable du traitement ne sont pas clairs. L'arrêté royal oblige en son article 31 le responsable à justifier lesdits motifs dans sa déclaration. Cette justification sera reprise dans le registre public des déclarations. L'arrêté royal précise aussi que le responsable – ou le tiers à qui les données ont été communiquées – doit néanmoins, lors de la première prise de contact avec la personne concernée, lui communiquer l'information prévue légalement [129].

La seconde exception vise les cas où l'enregistrement ou la communication sont effectués en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Son libellé élargit singulièrement la portée restreinte de l'exception prévue par la directive, sur laquelle l'exception belge prétend se fonder [130].

SECTION 2. L'OBLIGATION DE COMMUNICATION ET DE RECTIFICATION DES DONNÉES

570 **Généralités**

L'idée de transparence, qui est à la base de nombreuses dispositions de la loi, a notamment pour but de permettre à la personne concernée d'exercer elle-même un

128. Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, *Doc. Parl.*, Ch. repr., sess. ord. 1998-1999, n° 1566/10, p. 122, n° 26.
129. Article 30 de l'arrêté royal. L'arrêté royal rappelle également que des règles particulières ont été édictées concernant les traitements ultérieurs à finalité scientifique, statistique et historique.
130. Th. LÉONARD et Y. POULLET, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, p. 389, n° 46.

contrôle sur les traitements portant sur des données à caractère personnel qui la concernent.

La personne concernée a, en effet, le droit d'accéder à l'ensemble de ces données afin d'en obtenir, le cas échéant, la rectification. Ces droits sont cependant rarement exercés en pratique.

La loi prévoit aussi un droit de s'opposer au traitement des données dans les hypothèses et conditions qu'elle détermine.

La loi instaure une procédure d'accès indirect – c'est-à-dire exercée par l'intermédiaire de la Commission – pour les traitements poursuivis par certaines autorités publiques (police, sûreté de l'Etat, etc.) [131].

Sous-section 1. L'accès aux données

580 Portée

L'article 10 de la loi permet à toute personne concernée justifiant de son identité d'obtenir du responsable du traitement:

- la confirmation de l'(in)existence du traitement, ainsi que les finalités du traitement, les catégories de données traitées et de destinataires;
- la communication, sous une forme intelligible, des données traitées ainsi que toute information disponible sur leur origine; toutes les données qui font l'objet d'un traitement au sens de la loi sont ici visées (informations objectives, subjectives, photographies, etc.);
- la connaissance de la logique suivie lors du traitement en cas de système automatisé de décision [132].

Le responsable doit également rappeler dans sa réponse l'existence des droits de correction, du droit d'intenter une action en cessation et de consulter, le cas échéant, le registre public des déclarations.

590 Introduction de la demande d'accès

Afin d'obtenir l'accès aux informations précitées, la personne concernée doit adresser un courrier daté et signé au responsable du traitement. Elle peut aussi l'adresser à son représentant en Belgique ou à un de ses mandataires ou préposés, voire même au sous-traitant tenu alors de transmettre la demande au responsable [133].

La demande d'accès émane normalement de la personne concernée elle-même. Rien ne permet toutefois d'exclure l'hypothèse d'un mandat spécial donné à un tiers, notamment son avocat [134]. La personne concernée, qu'elle exerce son droit personnellement ou via un mandataire, doit justifier de son identité. Devant le silence de la

131. Visées à l'article 3, § 4 à § 6 de la loi. Les modalités concrètes de ce droit sont réglées par les articles 36 à 46 de l'arrêté royal.
132. Sur cet article, voir *supra* n° 500.
133. Article 32 de l'arrêté royal.
134. J. Dumortier, 'De verplichtingen van de houder van het best and' *in Personnsgegevens en privacybescherming Commentaar op de wet tot bescherming van de persoonlijke levensfeer*, *op. cit.*, p. 96; *Contra* mais à tort E. Meysmans, 'Het recht van toegang en verbetering in de Belgische privacywet', *op. cit.*, p. 226. L'auteur se fonde sur le texte de l'article 10 de la loi visant 'de hem betreffende gegevens die in een verwerking zijn opgenomen' (les données qu'un traitement contient à son sujet). C'est oublier que le mandataire agit au nom et pour compte de son mandant. Du reste, l'auteur admet que l'accès aux données soit exercé par un avocat.

loi, il est recommandé d'annexer à sa demande une copie *recto verso* de sa carte d'identité.

La demande peut être remise sur place ou transmise par voie postale, voire par tout autre moyen de télécommunication [135]. La personne concernée devra toutefois être attentive à se ménager la preuve de l'exercice de son droit. En cas de remise sur place, l'arrêté royal impose à la personne qui reçoit la demande de délivrer immédiatement un accusé de réception daté et signé.

Le responsable du traitement quant à lui sera attentif au contrôle de l'identité de la personne concernée: il ne peut en effet communiquer des données à caractère personnel à une personne non autorisée [136].

600 Réponse du responsable du traitement

Le responsable du traitement, ou toute autre personne désignée par le Roi, qui reçoit une demande d'accès dispose, à compter de la réception de la demande, d'un délai maximal de quarante cinq jours pour y donner une suite [137]. Toutefois, l'article 10, § 2 de la loi dispose que les renseignements doivent être communiqués sans délai, ce qui implique que tout soit mis en œuvre pour satisfaire au plus vite la demande, sous peine de voir engagée la responsabilité du responsable.

Cette suite consiste d'abord à vérifier la recevabilité de la demande d'accès. Le responsable n'est en effet pas tenu de répondre à une demande introduite alors qu'un délai raisonnable n'est pas expiré depuis une demande antérieure de la même personne à laquelle il a été répondu ou depuis la date de communication d'office des données demandées [138]. Le but du législateur est bien ici d'éviter certains abus consistant en des demandes répétitives ou intempestives de la même personne concernée.

Si la demande d'accès est recevable, le responsable du traitement est tenu de communiquer les informations prévues par la loi à la personne concernée. La communication des données doit se faire sous une forme compréhensible, sous peine de manquer au but du droit reconnu à la personne concernée, ce qui exclut un langage informatique ou un listing sous forme de codes sans autre explication. La loi ne prévoit cependant pas de forme particulière. Il est donc utile que le responsable du traitement se ménage une preuve de la communication des données.

610 Accès aux données relatives à la santé

Toute personne a droit également à prendre connaissance des données à caractère personnel traitées relatives à sa santé, soit directement, soit avec l'aide d'un praticien professionnel en soins de santé [139].

La communication elle-même des données peut être effectuée par l'intermédiaire d'un professionnel des soins de santé choisi par la personne concernée et cela, à la demande du responsable du traitement ou de la personne concernée.

L'exercice de ce droit d'accès a lieu sans préjudice de l'application de l'article 9, § 2 de la loi du 22 août 2002 relative aux droits du patient. Cette disposition organise l'accès du patient à son dossier médical selon des modalités distinctes de celles

135. Article 32 de l'arrêté royal.
136. *Cf. infra* n° 790 et 820.
137. Article 10, § 1er *in fine* de la loi.
138. Article 10, § 3 de la loi.
139. Article 10, § 2 de la loi.

analysées ici. Ces dispositions particulières s'appliquent indépendamment de la loi sur la protection des données.

Dans les circonstances et aux conditions strictes que la loi détermine, la communication des données relatives à la santé traitées pour une finalité de recherches médico-scientifiques peut être différée au plus tard jusqu'à l'achèvement des recherches. Il faut alors qu'il soit manifeste qu'il n'existe aucun risque d'atteinte à la vie privée de la personne concernée (1); que les données ne soient pas utilisées pour prendre des mesures à l'égard de cette personne (2); que ladite communication soit susceptible de nuire gravement auxdites recherches (3); que la personne ait donné son autorisation écrite et préalable quant au traitement et à la possibilité de différer la communication des données (4). Autant dire que cette exception, au vu de ces conditions, a peu de chances d'être mise en œuvre en pratique...

Sous-section 2. La rectification des données

620 Portée

L'article 12 de la loi prévoit que toute personne a le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel inexacte qui la concerne ainsi que la suppression ou l'interdiction d'utilisation des données qui, compte tenu du but du traitement, sont incomplètes ou non pertinentes ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui ont été conservées au-delà de la période autorisée.

Ce droit de rectification doit donc se comprendre au sens large. Il vise de manière générale toute difficulté relative à la qualité des données traitées – exactitude, pertinence, etc. – mais aussi à la légitimité et la licéité du traitement des données – interdiction de traitement, légitimité de la finalité, etc. –.

La charge de la preuve repose sur la personne concernée par les données, ce qui pose souvent en pratique une grande difficulté. Parfois, cette preuve sera même impossible, notamment si elle révèle une appréciation subjective du responsable du traitement. Dans cette dernière hypothèse, seul le caractère excessif de la donnée paraît pouvoir être contesté.

Contrairement aux cas où la loi ouvre un droit d'opposition, la suppression ou un effacement des données ne peuvent être obtenus par la personne concernée que si elle rapporte préalablement la preuve de la violation de la loi.

Dès la réception d'une demande de rectification, tout comme en cas de notification de l'introduction de l'instance visée à l'article 14, le responsable du traitement doit indiquer l'existence de la contestation lors de toute communication des données litigieuses à des tiers [140]. Cette mention doit apparaître jusqu'à ce qu'une décision judiciaire soit coulée en force de chose jugée.

630 Introduction de la demande de rectification et réaction du responsable du traitement

Dans les même formes que pour le droit d'accès, la personne concernée transmet sa demande de rectification au responsable du traitement ou aux autres personnes précitées [141]. La personne concernée ayant la charge de la preuve, la demande contiendra les motifs justifiant la correction ou la suppression des données litigieuses.

140. Article 15 de la loi.
141. Article 33 de l'arrêté royal.

Dans le mois de la demande, la rectification des données contestées est communiquée par le responsable du traitement tant à la personne concernée, qu'aux tiers auxquels les données ont été communiquées. Ces derniers ne reçoivent la rectification que « *pour autant que le responsable du traitement ait encore connaissance des destinataires de la communication* » et que « *la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés* ».

SOUS-SECTION 3. L'OPPOSITION AU TRAITEMENT

640 Portée

L'article 12, § 1er de la loi consacre le droit d'opposition dans deux hypothèses.

Dans la première hypothèse, la personne concernée a le droit de s'opposer au traitement de certaines de ses données pour des raisons sérieuses et légitimes tenant à une situation particulière. Le traitement est donc licite en lui-même (il poursuit une finalité légitime, il respecte le régime des données sensibles, etc.) mais il est néanmoins particulièrement dommageable à la personne concernée pour des raisons qui sont propres et dépendantes de sa situation particulière. Notons que la loi interdit ce droit d'opposition lorsque le traitement est nécessaire à la conclusion ou à l'exécution d'un contrat ainsi qu'au respect d'une obligation légale.

La seconde hypothèse est de loin la plus fréquente. Gratuitement et sans justification, la personne concernée peut s'opposer au traitement projeté lorsque des données à caractère personnel sont collectées à des fins de « *direct marketing* ».

L'effet d'une opposition fondée sur l'une ou l'autre des deux hypothèses est l'effacement des données litigieuses par le responsable du traitement.

650 Information de l'existence du droit d'opposition en matière de marketing direct

On a vu que le responsable du traitement devait informer la personne concernée de l'existence du droit d'opposition ouvert à son profit dans le cas de traitements à finalité de marketing direct [142].

L'arrêté royal est venu préciser les modalités particulières de cette information.

Soit le responsable du traitement obtient directement les données de la personne concernée, il doit alors offrir lors de cette collecte la possibilité de s'opposer gratuitement au traitement [143]. Si la collecte est effectuée par écrit, la personne doit pouvoir exercer son droit sur le document écrit (coupon-réponse dans un journal, formulaire de commande, voire formulaire électronique sur interne, etc.) [144]. Si la collecte est effectuée autrement que par écrit (par téléphone, carte à puce, etc.), le responsable doit l'inviter à exercer son droit d'opposition soit sur un document *ad hoc* qu'il lui communique dans les deux mois de l'obtention des données, soit par tout autre moyen technique lui permettant de garder une preuve que la personne concernée a eu la possibilité d'exercer son droit [145]. Dans ce dernier cas, l'invitation à l'exercice du droit doit être concomitante à l'obtention des données en vertu du prescrit de l'article 9, § 1er de la loi.

142. *Cf. supra*, no 530
143. Article 9, § 1er de la loi.
144. Article 34, alinéa 1er de l'arrêté royal.
145. Article 34, alinéa 2 de l'arrêté royal.

Soit le responsable du traitement a obtenu les données d'une personne autre que la personne concernée par les données. L'article 9, § 2 de la loi précise que l'information doit avoir lieu avant que les données ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de marketing direct. L'arrêté royal précise alors que le responsable doit prendre contact avec elle par écrit pour l'interroger sur ses intentions à l'égard de l'exercice du droit d'opposition.

660 Introduction de la demande d'opposition et réaction du responsable du traitement

La personne concernée transmet normalement sa demande d'opposition au responsable du traitement ou aux autres personnes précitées dans les même formes que pour le droit d'accès et de rectification [146]. Cela étant, elle pourra normalement utiliser les supports écrits parfois imposés pour l'informer de l'existence du droit.

Dans le mois de l'opposition, le responsable doit lui communiquer quelle suite il a réservé à sa demande. Si cette dernière est justifiée, il doit arrêter de traiter les données litigieuses.

SECTION 3. L'OBLIGATION DE DÉCLARATION DES TRAITEMENTS AUTOMATISÉS

SOUS-SECTION 1. LE PRINCIPE

670 Portée de l'obligation de déclaration

La loi organise une formalité de déclaration des traitements entièrement ou partiellement *automatisés* ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées. La déclaration doit être effectuée avant leur mise en œuvre effective. Le but est d'assurer une information claire et complète tant à la Commission de la protection de la vie privée qui y trouve un outil nécessaire à l'exercice de ses missions de contrôle qu'au citoyen qui y trouve des informations nécessaires à l'exercice de ses droits.

En vue d'optimaliser cette transparence, les différentes déclarations sont regroupées et consignées dans un registre, appelé communément « *fichier des fichiers* » [147]. Ce dernier reprend la liste des traitements automatisés et de leurs principales caractéristiques. Son accès au public est organisé conformément au prescrit des articles 63 à 69 de l'arrêté royal. Retenons simplement qu'il est accessible via le site internet de la Commission, lors d'une consultation sur place dans les locaux de la Commission ou par une demande orale ou écrite d'extraits.

La formalité de déclaration mise explicitement à charge du responsable du traitement ne concerne que les traitements *automatisés*. On peut se demander ce qu'il faut entendre par la référence, absente dans l'ancien texte, « *d'un ensemble de tels traitements ayant une même finalité ou des finalités liées* » et comment la comprendre au regard des concepts de « *traitement* » et de « *finalité* » [148]. Ce qui est certain, c'est

146. Article 12, § 2 de la loi.
147. Article 18 de la loi. Seules les indications reprises à l'article 17, § 3 et 6 sont visées.
148. Voir Th. LÉONARD et Y. POULLET, 'La protection des données à caractère personnel en pleine (r)évolution', *op. cit.*, pp. 392 et 393, n° 60 qui relèvent les incohérences du texte et l'opinion plus conciliante de D. DE BOT, *Verwerking van persoonsgegevens*, *op. cit.*, p. 267 et s.

que la loi a voulu alléger l'obligation de déclaration en permettant d'opérer une même déclaration pour différents finalités liées à un ou plusieurs traitements. On s'accordera à dire que ce sont les circonstances de fait qui seront déterminantes et qu'il faut veiller à trouver une relation factuelle évidente entre différents traitements et finalités pour opérer une seule déclaration [149].

La Commission a réglé la difficulté en proposant dans un lexique de finalités attaché à la déclaration des catégories de finalités dans lesquelles les finalités sont présumées liées [150]. Ainsi, par exemple, les finalités de gestion de la clientèle et de lutte contre la fraude et infractions de la clientèle sont rangées dans la même catégorie et considérées comme liées. Elles peuvent donc faire l'objet d'une seule et même déclaration.

La déclaration n'est pas une procédure d'autorisation de traitement mais une obligation purement administrative. En cas de plainte, de contrôle ou de procédure judiciaire, les informations reprises dans la déclaration seront censées correspondre à la réalité et feront foi contre le responsable du traitement. L'inexactitude ou le défaut d'informations exigées dans la déclaration sont érigés en infraction pénale [151].

La déclaration comporte une description des caractéristiques du traitement. Il s'agit essentiellement de l'identification du responsable du traitement, de la finalité ou de l'ensemble des finalités liées du traitement, et des catégories de personnes admises à obtenir les données [152]. Deux situations donneront lieu à un complément de déclaration. D'une part, lorsque la Commission de la protection de la vie privée effectue une démarche à cet effet [153] et, d'autre part, lorsque les données traitées sont destinées à être transmises *vers l'étranger* [154].

Si le traitement vient à être supprimé ou si une des mentions de la déclaration devait être modifiée, une déclaration *ad hoc* est requise [155]. Il en est ainsi lorsque les données sont traitées en vue d'une finalité différente de celle prévue dans une première déclaration.

Dans les trois jours ouvrables de la réception d'une déclaration, la Commission adresse un accusé de réception [156].

680 Montant et paiement de la redevance

En son paragraphe 9, l'article 17 de la loi prévoit que le responsable du traitement est tenu de verser une contribution au profit de la Commission lors de chaque déclaration.

Les articles 47 à 50 de l'arrêté royal exécutent cette dernière disposition.

Le montant des redevances est fonction du type de déclaration choisi par le responsable du traitement:

a. la redevance pour la déclaration effectuée au moyen d'un formulaire papier fourni par la Commission est fixée à 125 euros;

149. *Idem*.
150. Ce document, ainsi que les déclarations et toutes les explications utiles quant à la procédure de déclaration sont disponibles librement et gratuitement sur le site de la Commission de la protection de la vie privée (http://www.privacy.fgov.be).
151. Article 39, 8° de la loi.
152. Le détail des mentions est repris à l'article 17, § 3 de la loi.
153. Article 17, § 4. Le complément de déclaration portera en particulier sur l'origine des données, de la technique d'automatisation choisie et des mesures de sécurité prévues.
154. Article 17, § 6. Doivent alors être mentionnées les catégories de données faisant l'objet de la transmission et le pays de destination pour chaque catégorie de données.
155. Article 17, § 7 de la loi.
156. Article 17, § 2 de la loi.

b. la redevance pour la déclaration effectuée au moyen du formulaire type sur support magnétique fourni par la Commission est fixée à 25 euros; il en est de même pour la déclaration effectuée via Internet, qui est assimilée par la Commission à une déclaration sur support magnétique.
c. la redevance pour une déclaration modificative d'une déclaration initiale est fixée à 20 euros.

Le responsable effectue le paiement des redevances au moyen des documents mis à disposition par la Commission. La contribution due doit en pratique être versée sur le compte n° 679-2005601-29 de la Commission de la protection de la vie privée à 1000 Bruxelles, avec communication du numéro du dossier HM c'est-à-dire le numéro attribué au responsable du traitement.

Il convient de noter que le responsable paye un seul et même montant pour toutes les informations qu'il déclare à la même occasion.

690 Déclarations-types élaborées par la Commission

Pour l'instant, trois régimes de déclaration sont proposés par la Commission. L'un est général et concerne la quasi-totalité des traitements. Le second concerne les déclarations standard qui ont été mises au point par la Commission et des organisations professionnelles, sectorielles ou des secrétariats sociaux. Le troisième est propre aux traitements ultérieurs à finalités scientifiques, statistiques et historiques.

Les modèles types de déclaration créés par la Commission sont tous composés de quatre parties. La première comprend les données d'identification du responsable du traitement, la seconde celles relatives au traitement. La troisième est propre aux modifications apportées dans un traitement ayant fait l'objet d'une déclaration antérieure et la quatrième à la suppression d'un tel traitement.

Toutes les mentions prévues par la loi s'y retrouvent.

Le responsable du traitement voit sa tâche facilitée par l'existence de lexiques et notices explicatives. Les lexiques reprennent par exemple les catégories de données et les finalités les plus courantes. Mais ces documents, quoique très utiles, ne peuvent être complets et le responsable doit toujours apporter les précisions qui s'imposent dès lors que son traitement diffère des indications qui lui sont données.

Sous-section 2. Les exceptions à l'obligation de déclaration

700 Généralités

En application de l'article 17, § 8 de la loi, le Roi a reçu le pouvoir d'exempter de déclaration les traitements automatisés qui ne présentent manifestement pas d'atteinte à la vie privée. L'arrêté royal [157] accorde cette exemption à douze catégories de traitements qui répondent, éventuellement sous certaines conditions, au critère légal d'exemption. Seules les exemptions intéressant normalement l'entreprise seront développées ci-après [158]. Il est à noter que ces exemptions sont quasi identiques à

157. Articles 51 à 62.
158. Parmi celles qui ne feront pas l'objet d'un commentaire, on citera seulement les traitements effectués par une fondation, une association ou tout autre organisme sans but lucratif dans le cadre de leurs activités ordinaires (art. 56 de l'arrêté royal). Le lecteur recherchant de l'information sur les exemptions relatives à une entreprise ne relevant pas du secteur privé est dès lors invité à consulter l'arrêté royal.

celles issues de l'ancien texte. C'est pourquoi l'on se réfère encore utilement ci-après à l'exposé des motifs de l'ancien arrêté royal.

La déclaration étant de principe, l'exemption représentant l'exception, une interprétation restrictive des finalités déterminées par le Roi paraît s'imposer. Ces dernières restreignent en effet la portée du principe de transparence, au cœur de la protection accordée par la loi aux libertés individuelles de la personne concernée par les données.

710 Traitements relatifs à l'administration des salaires

L'article 51 de l'arrêté royal prévoit une exemption de déclaration pour les traitements automatisés relatifs à l'administration des salaires.

Pour ces types de traitement automatisé, les données se rapportent à des personnes « *au service du ou travaillant pour le responsable du traitement* ». Le statut du bénéficiaire (salarié, statutaire, indépendant, etc.) est ici sans importance [159].

Le rapport au Roi précise que le terme « salaire » comprend toutes formes de salaire, traitement ou autres rémunérations pour ou en rapport avec des prestations effectuées par les intéressés à la demande ou pour le responsable du traitement. La nature de la rémunération (remboursement de frais, salaire, etc.) est sans importance.

L'arrêté est, par contre, muet quant aux buts d'utilisation des données que recouvre l'administration des salaires. On peut notamment y inclure les opérations de calcul et de paiement des rémunérations, les calculs de cotisations de toute nature donnant lieu à des retenues (pension, sécurité sociale, mutuelle, etc.), les déclarations et communications d'informations aux administrations concernées, la gestion des retenues sur salaires imposées par des tiers légitimes (saisies-arrêts sur salaires, etc.), etc. Le rapport au Roi paraît identifier l'administration des salaires aux tâches éventuellement confiées aux secrétariats sociaux. C'est oublier que ces derniers remplissent souvent des missions plus larges comme certains aspects de l'administration du personnel ou du conseil juridique.

Sous réserve du contrôle du caractère de nécessité par rapport aux types d'opérations précitées, les catégories de données traitées peuvent être très diverses. D'après le rapport au Roi, « *l'exemption concerne le traitement de toutes les données qui sont requises par la loi sur les documents sociaux et les obligations complémentaires et qui découlent notamment des dispositions en matière de droit du travail, de sécurité sociale, de législation fiscale y compris les dispositions des conventions collectives et individuelles de travail* » [160]. On retrouvera donc des données d'identification, financières, administratives (composition de famille, affiliation à une mutuelle, ...), etc.

Le Rapport au Roi admet explicitement que certaines données sensibles au sens de la loi, notamment des données judiciaires [161], puissent être traitées dans le cadre de la gestion des salaires tout en bénéficiant de l'exemption.

Pour bénéficier de l'exemption, les données ne peuvent être utilisées pour une autre finalité que l'administration des salaires, ce qui réduit fortement la portée de l'exemption. En effet, une grande partie de ces données sera toujours, par exemple, traitée en vue de la gestion du personnel, pour ne citer que cet exemple. En outre, ces données doivent uniquement être communiquées aux destinataires « qui en ont droit ». Le Roi paraît viser par là les destinataires à qui les données doivent être communiquées

159. Rapport au Roi précédant l'arrêté royal n° 13, *M.B.*, 15 mars 1996, p. 5805.
160. *Idem*, p. 5805.
161. Le Rapport au Roi vise explicitement des données relatives à la détention préventive et, plus généralement, les données judiciaires qui ont une incidence sur le contrat de travail (p. 5805).

(administrations de la sécurité sociale, etc.). Enfin, elles ne peuvent être conservées au delà du temps nécessaire à la poursuite des finalités du traitement.

720 Traitements relatifs à l'administration du personnel

Les traitements relatifs à l'administration du personnel sont également exemptés de l'obligation de déclaration.

Le Rapport au Roi énonce qu'il faut entendre par là « *les traitements relatifs au personnel effectués par les employeurs, pour autant que lesdits traitements ne découlent pas directement de l'application de dispositions légales, réglementaires ou conventionnelles concernant l'emploi* » [162]. Le Roi paraît identifier ces derniers traitements à ceux nécessaires à l'administration des salaires.

Cette « définition » paraît *a priori* excessivement large par rapport au texte même de l'arrêté et provoque un trouble quant à la délimitation des traitements qui relèvent de l'administration des salaires ou du personnel. En effet, la presque totalité des relations entre un salarié et son employeur tombe directement sous le coup de réglementations ou de dispositions conventionnelles. Est-ce à dire que les traitements utilisés aux fins de la gestion de ces relations « réglementées » visent automatiquement l'administration des salaires? La question n'est pas sans intérêt pratique puisqu'on verra que les conditions d'exemption sont plus lourdes pour les finalités propres à l'administration du personnel.

L'administration des salaires au sens large comprend, selon nous, toutes les finalités ayant un rapport direct avec la gestion des rémunérations généralement quelconques versées au bénéficiaire dans le cadre de la relation de travail ou de la prestation effectuée. C'est un fait que la matière est soumise à de nombreuses obligations administratives imposées par la loi ou des arrêtés réglementaires. Toute la relation de travail ou d'emploi ne se résume pas, loin s'en faut, au paiement d'une rémunération et à son administration.

Si l'on sort de l'administration du salaire, on sort du champ d'application de l'article 51 de l'arrêté royal et on entre dans celui de l'article 52, à savoir l'administration du personnel. Cette dernière est donc une notion générique qui couvre toutes les finalités de traitements automatisés poursuivies à l'occasion de la relation de travail, excepté celles relatives à l'administration du salaire.

L'article 52 recouvre donc des finalités de traitements ayant trait notamment à la sélection et au recrutement, à la formation, à l'organisation ou à l'évaluation du travail mais aussi à des communications de données aux administrations ou des tiers dès lors que cette communication ne présente pas de lien direct avec la gestion du salaire.

L'exemption relative à la déclaration des traitements poursuivant des finalités d'administration du personnel est conditionnelle.

Le traitement ne peut se rapporter à des données relatives à l'état de santé de la personne concernée par les données. Le traitement ne peut pas non plus porter sur des données sensibles et/ou judiciaires au sens des articles 6 et 8 de la loi, ni sur des données destinées à une évaluation de l'intéressé. Cette condition imposera donc la déclaration de la plupart des traitements automatisés poursuivis en vue de l'embauche et de la sélection du personnel ainsi que ceux effectués à des fins de planification de carrière.

Enfin, les données traitées ne peuvent être communiquées à des tiers, sauf exceptions: le traitement est poursuivi dans le cadre de l'application d'une disposition

162. Rapport au Roi précédant l'arrêté royal n° 13, *op. cit.*, p. 5805.

légale ou réglementaire ou les communications sont indispensables à la réalisation des objectifs du traitement.

L'arrêté rappelle également que les données ne peuvent être conservées au-delà du délai nécessaire à la finalité poursuivie.

730 **Traitements relatifs à la comptabilité**

L'article 53 de l'arrêté royal admet l'exemption de déclaration pour les traitements « *qui se rapportent exclusivement à la comptabilité du maître du fichier, pour autant que lesdites données soient utilisées exclusivement à la comptabilité* ».

Le rapport au Roi précise que le terme « comptabilité » doit être interprété « *dans le sens de la loi du 17 juillet 1975 relative à la comptabilité et aux comptes annuels des entreprises comme étant l'administration qui, tenue de manière régulière et conformément aux règles usuelles en la matière, peut servir de moyen de perception et de contrôle lors de la perception des impôts étant entendu que l'ouverture et la communication des documents peuvent être demandées au tribunal* » [163]. Le Ministre précise, en outre, que « *toute comptabilité répondant à cette définition, qu'elle tombe ou non sous le champ d'application de la loi du 17 juillet 1975, est susceptible d'obtenir une exemption. La référence à la loi précitée concerne dès lors uniquement la définition de la notion de comptabilité* ».

Les conditions de l'exemption sont que les données soient utilisées exclusivement à la comptabilité du responsable; que ces données portent uniquement sur des personnes dont les données sont nécessaires à la comptabilité [164]; la non-communication des données aux tiers, sauf si la communication a lieu en application d'une disposition légale ou réglementaire ou si elle est indispensable à la tenue de la comptabilité. Rentre vraisemblablement dans cette dernière hypothèse, la communication des données à un service comptable externe à l'entreprise.

Enfin, les données ne peuvent être conservées au-delà du délai nécessaire à la comptabilité et à l'archivage.

740 **Traitements relatifs à l'administration des données d'actionnaires et d'associés**

Bénéficient de l'exemption, en application de l'article 54 de l'arrêté royal, les traitements « *qui visent exclusivement l'administration d'actionnaires et d'associés* ».

Le rapport au Roi précise que sont visées les opérations relatives à l'enregistrement des associés et actionnaires, à la gestion des bénéfices financiers et autres, aux convocations, aux procès-verbaux, etc. [165].

Les finalités des traitements en cause ne font l'objet d'aucune autre précision. Les traitements visés sont ceux portant sur les associés et actionnaires du responsable du traitement et des sociétés membres d'un groupe dont il ferait partie. Sont par contre exclues du bénéfice de l'exemption les banques de données qui reprendraient des renseignements relatifs aux actionnaires et associés de toutes ou partie des sociétés belges ou étrangères [166].

Les conditions de l'exemption sont la non-communication à des tiers sauf dans le cadre de l'application d'une disposition légale ou réglementaire [167]. Si les données sont donc transmises aux banques de données commerciales dont il est question ci-

163. Rapport au Roi, p. 5806.
164. Cette précision est inutile puisque le principe de conformité des donnée a le même effet.
165. Rapport au Roi, p. 5806.
166. *Idem*.
167. Le Roi rappelle que les données ne peuvent être conservées au-delà du délai nécessaire à l'objectif visé.

avant, le traitement perd le bénéfice de l'exemption. Le nouveau texte précise que le traitement doit porter uniquement sur les données nécessaires à l'administration d'actionnaires et d'associés et que ces données soient uniquement relatives à des personnes dont les données sont nécessaires à cette administration. Là encore, il s'agit d'une simple application des principes de légitimité et de conformité tels qu'explicités ci-avant.

750 Traitements relatifs à la gestion de la clientèle et des fournisseurs

La gestion de la clientèle et celle des fournisseurs fait l'objet d'une exemption prévue à l'article 55 de l'arrêté royal.

Le traitement peut uniquement porter sur des clients ou des fournisseurs potentiels, existants ou anciens du responsable du traitement. Elle vise, d'après le Ministre, la gestion de toutes les relations commerciales du responsable du traitement, indépendamment de sa qualité (entreprise, profession libérale, etc.) [168].

Pour bénéficier de l'exemption, le traitement ne peut porter sur des données relatives à la santé de l'intéressé, ni sur des données sensibles ou judiciaires au sens des articles 6 et 8 de la loi.

Les données ne peuvent être communiquées à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou aux fins de la gestion normale de l'entreprise.

Pour la seule gestion de la clientèle, aucune donnée ne peut être enregistrée dans un traitement sur la base d'informations obtenues de tiers. Le Ministre vise explicitement dans son commentaire l'hypothèse de données sur des clients potentiels obtenues auprès de clients (action de parrainage). Il ajoute que l'exemption reste de mise dans le cas de données obtenues de sources externes publiques [169]. Cette dernière interprétation paraît sans fondement. La notion de tiers ne prévoit pas une distinction en fonction de l'origine des données à caractère personnel.

Ici aussi, le texte précise que les données ne peuvent être conservées plus longtemps qu'il n'est nécessaire à la gestion normale de l'entreprise.

760 Traitements visant l'identification indispensable à la communication

L'article 57 de l'arrêté exempte de déclaration les « *traitements de données d'identification indispensables à la communication effectués dans le seul but d'entrer en contact avec l'intéressé* ».

Cette disposition vise, de manière générale, à exclure de la déclaration les traitements de données d'identification utilisées par le responsable du traitement pour nouer ou entretenir des relations publiques, sociales ou professionnelles [170]. On peut penser, par exemple, aux traitements effectués en vue d'adresser des invitations à une conférence ou à une réunion de travail. C'est ce que l'on appelle communément les « fichiers d'adresses ». Les données sont relatives au nom, à l'adresse, à l'entreprise, à la fonction, au titre, à la langue, au numéro de téléphone et de téléfax, à l'adresse électronique, etc. des personnes avec lesquelles on désire entrer en contact. Bref, selon l'expression de la Commission, il s'agit de toutes les données d'identification et de localisation de la personne dans l'espace et dans le temps [171].

168. Rapport au Roi, p. 5806.
169. Rapport au Roi, p. 5807.
170. *Idem*.
171. Avis 33/95 du 22 décembre 1995 de la Commission, *M.B.*, 15 mars 1996., p. 5814.

Tant le Ministre que la Commission précisent cependant qu'aucune autre donnée ne peut être utilisée pour bénéficier de l'exemption. Sont donc exclus les traitements portant sur des données déterminant un profil ou relatives aux hobbies, aux préférences, aux habitudes de consommation, etc. des personnes concernées.

La disposition ne jouera qu'à titre subsidiaire. Les traitements précités ne bénéficient de l'exemption que s'ils ne sont pas déjà visés par d'autres dispositions de l'arrêté. Paraissent donc exclus du bénéfice de l'exemption les traitements de communication qui seraient visés par d'autres dispositions de l'arrêté mais qui ne rempliraient pas les conditions spécifiques d'exemptions prévues. On pense par exemple aux traitements de données relatives à l'administration de la clientèle, des fournisseurs, etc. qui seraient obtenues de tiers [172].

Les données utilisées ne peuvent toutefois pas être communiquées à des tiers. Si le responsable commercialise ou échange ses fichiers d'adresses, il ne bénéficie pas de l'exemption.

770 Traitements relatifs à l'enregistrement des visiteurs dans le cadre d'un contrôle d'accès

L'article 58 de l'arrêté exempte également de l'obligation de déclaration les traitements portant exclusivement sur l'enregistrement de visiteurs, effectué dans le cadre d'un contrôle d'accès.

Les conditions sont ici très strictes puisque seules peuvent être traitées les données relatives aux noms, à l'adresse professionnelle du visiteur, à l'identification de son employeur et de son véhicule, au nom, à la section et à la fonction de la personne visitée ainsi qu'au jour et à l'heure de la visite.

De plus, seule la finalité de contrôle de l'accès est visée, à l'exclusion de toute autre, et les données ne peuvent être utilisées que pour cette finalité. Est donc, par exemple, exclu de l'exemption un contrôle de l'emploi du temps de la personne visitée par l'employeur. Le Ministre et le Roi ont toutefois précisé que le contrôle de l'accès peut englober aussi bien le contrôle au moment de la visite que les vérifications faites par la suite dans le cadre de la politique de sécurité interne [173].

SECTION 4. LES OBLIGATIONS DE SÉCURITÉ ET DE CONFIDENTIALITÉ

780 Généralités

La loi, en son article 16, vient définir des obligations de sécurité et de confidentialité à l'égard des traitements que le responsable du traitement met en œuvre. Certaines sont générales et d'autres particulières à certaines mesures concrètes et organisationnelles que la loi détermine. Ces obligations feront l'objet de contrôles par la Commission ou, le cas échéant, par les autorités judiciaires.

Une attention particulière est portée sur la relation de sous-traitance nouée par le responsable du traitement.

172. D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 290, n° 398.
173. Rapport au Roi, p. 5607.

790 Obligation générale de sécurité [174]

Le responsable du traitement, ou son représentant en Belgique, mais aussi le sous-traitant, sont tenus de prendre les mesures techniques et organisationnelles requises pour «*protéger les fichiers contre la destruction accidentelle ou non autorisée, contre la perte accidentelle, ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel*» [175].

Cette obligation vise les mesures de sécurité tant techniques qu'organisationnelles qui doivent être prises pour assurer le respect de la loi. Le piratage du système informatique par des tiers mais aussi les malveillances possibles des membres du personnel doivent être évités. A cet égard, on peut conseiller au responsable du traitement d'insérer tant dans ses contrats de travail que dans les contrats de services qui le lient à des tiers prestataires, une clause spéciale de confidentialité.

Le degré de protection doit être adéquat eu égard, d'une part, à l'état de l'art en la matière et aux dépenses suscitées par les mesures adoptées, et d'autre part, aux menaces virtuelles et à la nature des données à protéger [176, 177]. On peut s'interroger sur l'interprétation à donner à la notion de «*dépenses suscitées*». Faudra-t-il les évaluer au regard des moyens du responsable du traitement? Si l'on retient ce critère, la sécurité des données pourrait être plus ou moins bien assurée en fonction de la capacité financière du responsable du traitement.

800 Gestion de la relation de sous-traitance

Lorsque le traitement est confié en tout ou partie à un sous-traitant, le responsable ou, le cas échéant, son représentant, est soumis à diverses obligations particulières.

Il doit d'abord choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives au traitement. Cette obligation impose, selon nous, que le responsable s'informe des mesures qui seront prises par le sous-traitant et qu'il les évalue à la mesure de l'obligation de sécurité telle que définie par la loi [178]. Par le biais de cette obligation, il pourra le cas échéant voir sa responsabilité personnelle engagée au cas où celle du sous-traitant le serait suite à une méconnaissance de l'obligation de sécurité qui pèse également sur lui en vertu de la loi.

Il doit ensuite veiller au respect de ces mesures par le sous-traitant, notamment par la stipulation de mentions contractuelles. Le plus simple est d'annexer au contrat une description des mesures de sécurité techniques et organisationnelles auxquelles s'engage le sous-traitant. Les parties peuvent aussi prévoir des procédures de contrôle durant l'exécution du contrat (audit, etc.).

Le contrat doit fixer la responsabilité du sous-traitant à l'égard du responsable du traitement. Les parties peuvent ainsi modaliser la responsabilité contractuelle du sous-traitant conformément au droit commun. Il faut cependant être attentif au fait que plus la responsabilité du sous-traitant sera allégée, plus des doutes légitimes pourront naître quant au caractère raisonnable du choix du responsable du traitement. En effet, quelle

---

174. Pour plus de précisions, voir D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, pp. 247 et 254 et réf. citées.
175. Article 16, § 4 de la loi.
176. Des normes appropriées pour toutes ou certaines catégories de traitements pourront être édictées par le Roi sur avis de la Commission de la vie privée. Aucune réglementation particulière n'existe à l'heure actuelle.
177. Voir J.-P. Buyle, L. Lannoye, Y. Poullet, V. Willems, 'Le droit de l'informatique Chronique de jurisprudence (1987-1994)', *op. cit.*, p. 237, n° 74.
178. *Cf. supra*, n° 790.

est la valeur des garanties de sécurité censées être promises par le sous-traitant s'il n'admet qu'une responsabilité très limitée en cas de violation de ses obligations?

La loi demande également de convenir avec le sous-traitant que ce dernier n'agira que sur la seule instruction du responsable et qu'il sera tenu par les mêmes obligations de sécurité que celles auxquelles le responsable est tenu. Ce faisant, les obligations légales qui pèsent déjà sur le sous-traitant – et le responsable – en vertu de l'article 16, § 3 de la loi, sont contractualisées de sorte que leur non-respect par le sous-traitant risque également d'engager sa responsabilité contractuelle vis-à-vis du responsable.

Enfin, la loi impose que le contrat soit consigné par écrit ou sur un support électronique [179].

810 Mise à jour et rectification des données

L'article 4, § 1er, 4° de la loi, qui énonce le principe de finalité, précise déjà que les données à caractère personnel traitées doivent être exactes et si nécessaire mises à jour. L'article 16, § 1er, 3° de la loi précise et renforce l'obligation du responsable du traitement non seulement tenu de « *faire toute diligence pour tenir les données à jour* » et « *pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes* » mais cette dernière obligation est étendue aux données « *obtenues ou traitées en méconnaissance des articles 4 à 8* » de la loi (principe de finalité et régime des données sensibles).

Quelle est la portée de cette disposition ? Elle confirme *a priori* que les obligations de mise à jour, de rectification et de suppression sont considérées comme analogues à des obligations de moyen [180]. La jurisprudence avait, sous l'ancienne loi, entériné l'analyse [181]. Pourtant, le doute s'installe du fait de l'introduction de l'article 15*bis* et du retournement de charge de la preuve qu'il implique, selon certains [182].

820 Limitations de l'accès aux données

Le responsable du traitement doit veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limitées à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou les nécessités du service [183].

On vise donc ici les membres du personnel du responsable du traitement. Le critère de l'accès est la fonction exercée. Si l'accès n'est pas nécessaire à l'exercice de la fonction, il doit être dénié. Le responsable doit en outre veiller à ce que ces personnes autorisées ne puissent effectuer des traitements de données non nécessaires à leurs fonctions ou aux nécessités du service. Il doit ainsi veiller à ce qu'elles ne puissent effectuer des modifications, ajouts, effacements, lectures, rapprochements ou interconnexions non autorisés ou interdits au regard de ce critère.

L'article 16, § 3 de la loi précise encore que toute personne agissant sous l'autorité du responsable, du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement.

---

179. *Cf.* D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 260 et s. ainsi que le modèle de contrat qu'il propose en annexe de son ouvrage.
180. *Ibidem*, p. 255, n° 352.
181. Voir notamment, la jurisprudence analysée in Y. Poullet, A. Cruquenaire, N. Daubies *et alii*, *Droit de l'informatique et des technologies de l'information Chronique de jurisprudence 1995-2001*, *op. cit.*, p. 157, n° 159.
182. *Ibidem*.
183. Article 16, § 2, 2° de la loi.

830 Conformité des programmes aux mentions de la déclaration

L'article 16, § 2, 2° de la loi prévoit que le responsable du traitement doit s'assurer de la conformité des programmes servant aux traitements automatisés avec les termes de leur déclaration éventuelle.

Il est difficile de comprendre la portée exacte de cette obligation. Le responsable doit d'évidence veiller à ce que la déclaration vise effectivement les diverses utilisations possibles des données permises par le traitement automatisé.

840 Information du personnel

Le responsable du traitement est tenu de faire connaître aux personnes agissant sous son autorité – principalement les membres de son personnel – la teneur de la nouvelle loi ainsi que toute autre prescription pertinente relative aux exigences particulières de la vie privée face aux traitements de données à caractère personnel [184].

184. Article 16, § 2, 3° de la loi.

Chapitre 5. Le contrôle de l'application de la loi

850 **Généralités**

Le contrôle de l'application de la loi est exercé de diverses manières. Il revient en premier lieu à la personne concernée par les données qui exerce les droits qui lui sont reconnus par la loi. Le juge pénal peut également connaître des violations des nombreuses dispositions constitutives d'infractions (*cf. infra*, chapitre 6).

On s'attardera ci-après sur les pouvoirs de contrôle reconnus à la Commission de la protection de la vie privée et sur la procédure spécifique dont dispose la personne concernée devant le Président du tribunal de première instance. Un mot sera dit également sur la problématique de la mise en cause de la responsabilité civile du responsable du traitement depuis l'introduction dans la loi du nouvel article 15*bis*.

SECTION 1. LA COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE

860 **Généralités**

La loi a mis en place, sans préjudice de la compétence des autorités judiciaires, une autorité particulière, la Commission de la protection de la vie privée, ayant notamment pour mission le contrôle du respect de la loi.

La composition [185] de la Commission, comme son mode de fonctionnement [186], ont été modifiés par la loi du 26 février 2003 afin de lui donner une plus grande efficacité et une plus grande indépendance vis-à-vis des autres pouvoirs. Elle est instituée auprès de la Chambre. Elle comprend des comités sectoriels compétents pour instruire et statuer des demandes relatives au traitement ou à la communication de données faisant l'objet de législations particulières, dans les limites déterminées par celles-ci [187].

La Commission a reçu des missions administratives. Elle gère les déclarations des traitements automatisés que les responsables de traitement lui transmettent. Sur la base de ces déclarations, elle tient un « fichier des fichiers » [188], conçu pour permettre de donner aux personnes concernées ainsi qu'aux tiers une vue d'ensemble des traitements de données à caractère personnel en Belgique [189].

---

185. Articles 23 et 24 de la loi. Ses membres sont désignés par la Chambre. Huit sont effectifs, huit sont suppléants. Ils doivent offrir toutes les garanties leur permettant d'exercer leur mission avec indépendance et toutes les garanties de compétence dans le domaine de la protection des données. Il doit exister en son sein un équilibre entre les différents groupes socio-économiques (art. 24, § 4 de la loi). Le Président doit être magistrat (art. 24, § 1er de la loi). Ils sont élus sur des listes comprenant, pour chaque mandat à pourvoir, deux candidats présentés par le Conseil des Ministres.
186. Les membres sont élus pour une durée de six ans renouvelable (art. 24, § 4 de la loi). Si les membres peuvent être relevés de leur charge par la Chambre qui les a nommés en cas de manquement à leurs devoirs ou d'atteinte à la dignité de leur fonction, ce ne peut en aucun cas l'être à l'occasion des opinions qu'ils émettent ou des actes qu'ils accomplissent pour remplir leurs fonctions (art. 24, § 3 et § 6 de la loi). Dans les limites de leur attribution, les membres ne reçoivent d'instructions de personne.
187. Article 31*bis* de la loi.
188. Article 18 de la loi.
189. Cette vue d'ensemble sera fortement limitée vu le grand nombre d'exemptions de déclarations prévues par l'arrêté royal.

La Commission a également reçu une mission générale de proposition et de conseil à l'égard des pouvoirs publics. Elle est amenée à rendre des avis ou des recommandations, soit d'initiative, soit sur demande du Gouvernement, du Parlement, des exécutifs et conseils communautaires et régionaux ou d'un comité de surveillance. Ceux-ci portent sur toute question intéressant la protection de la vie privée à l'égard des traitements de données à caractère personnel [190].

870 Pouvoirs de contrôle de la Commission

Ce qui importe le plus dans le cadre de l'application de la loi à l'entreprise est la compétence générale de contrôle de son application reconnue à la Commission.

Cette dernière examine les plaintes qui lui sont adressées dans le cadre de ses missions. Cet examen est mené sans préjudice de toute voie de recours devant les tribunaux [191]. Si la Commission estime la plainte recevable, elle accomplit toute mission de médiation qu'elle juge utile [192]. Une plainte déposée à la Commission ne peut avoir pour conséquence une prise de décision contraignante vis-à-vis du responsable du traitement. La Commission ne peut que prendre un avis ou une recommandation négative vis-à-vis du responsable du traitement [193]. Elle ne peut toutefois contraindre ce dernier à respecter la loi. Elle communique ses décisions, avis ou recommandations au plaignant, au responsable et à toutes les autres parties à la cause. Elle adresse copie au Ministre de la Justice.

Il ne faut pas sous-estimer le poids de la Commission qui peut donner à l'exercice de ses missions une certaine publicité mettant l'entreprise dans une position délicate, notamment vis-à-vis de sa clientèle, voire de ses concurrents. Il convient à ce propos de rappeler que les avis et recommandations de la Commission sont publiés sur son site internet [194] et qu'elle émet parfois d'initiative des communiqués de presse sur certains dossiers. Elle fait annuellement rapport à la Chambre [195]. Elle peut également transmettre les dossiers litigieux à la justice. La Commission doit ainsi dénoncer au procureur du Roi les infractions dont elle aurait connaissance [196] et peut saisir d'initiative le tribunal de première instance de tout litige relatif à l'application de la loi ou de ses arrêtés royaux d'exécution [197].

La Commission a enfin reçu des pouvoirs d'investigation importants pour l'exécution de ses missions. Elle peut faire opérer des contrôles et vérifications en entreprise et est habilitée à requérir le concours d'experts [198]. Dans ce cas, les membres de la Commission ont la qualité d'officier de police judiciaire, auxiliaire du procureur du Roi [199]. Elle a également reçu le pouvoir d'exiger qu'une information complète lui soit transmise notamment sur l'origine des données traitées, la technique d'automatisation retenue et les mesures de sécurité prévues [200]. Ces pouvoirs sont d'autant plus importants que la loi érige en infraction pénale le fait d'empêcher la Commission

190. Article 30 de la loi.
191. Article 31, § 1er de la loi.
192. Article 31, § 3 de la loi.
193. *Idem*.
194. http://www.privacy.fgov.be
195. Article 32, § 2 de la loi.
196. Article 32, § 2 de la loi.
197. Article 32, § 3 de la loi.
198. Article 32, § 1er de la loi.
199. Article 32, § 1er de la loi.
200. Article 17, § 4 de la loi.

d'effectuer des vérifications ou de refuser de lui transmettre les informations demandées [201].

La Commission de la protection de la vie privée est donc une autorité qui est devenue incontournable vis-à-vis des entreprises qui poursuivent un grand nombre de traitements de données à caractère personnel ou traitent des catégories de données ayant un caractère sensible.

SECTION 2. LE PRÉSIDENT DU TRIBUNAL DE PREMIÈRE INSTANCE

880 Action en cessation – Généralités

La personne concernée par les données bénéficie d'un recours spécifique auprès du Président du tribunal de première instance siégeant comme en référé [202]. Le Président exerce donc une compétence au fond mais dans les formes accélérées du référé.

La juridiction présidentielle connaît « *de toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou encore qui a été conservée au-delà de la période autorisée* ».

De manière générale, on peut y voir une action en cessation permettant de demander de mettre fin à une violation de la loi [203], ce qui exclut toutefois l'octroi de dommages et intérêts [204]. Contrairement à d'autres actions en cessation, le principe selon lequel « le pénal tient le civil en état » trouve à s'appliquer en la matière [205].

Le Président peut, outre la cessation, ordonner au responsable du traitement d'informer les tiers à qui ont été communiquées les données, de leur rectification ou de leur suppression [206]. Saisi par requête unilatérale, il peut ordonner toute mesure de nature à éviter une dissimulation ou une disparition d'un élément de preuve [207]. L'ordonnance rendue par le tribunal est prononcée en audience publique et est exécutoire par provision nonobstant opposition ou appel [208].

---

201. Article 39, 10° et 13° de la loi.
202. Article 14 de la loi.
203. Sur cette action, voir P. LEMMENS, 'De procedure zoals in kort geding betreffende de bescherming van de persoonlijke levensfeer', *in Le développement des procédures 'comme en référé' De ontwikkeling van de procedures 'zoals in kort geding'*, Actes du colloque tenu à Louvain-la-Neuve le 17 décembre 1993, Bruxelles-Diegem, Bruylant-Kluwer, 1994, pp. 175 à 183; Th. LÉONARD, observations sous Civ. Bruxelles, Prés., 22 mars 1994, *J.T.*, 1994, pp. 843 à 847.
204. Civ. Bruxelles (Prés.), 19 décembre 2000, *Bull. ass.*, 2001, p. 266 et s. et note Ch. VAN OLDENEEL; Civ. Bruxelles (Prés.), 12 avril 1995, inédit, cité *in* Th. LÉONARD, 'Centrales de crédit et protection de la vie privée: incertitude et insécurité juridique', note sous Civ. Bruxelles (Prés.), 13 septembre 1995, *D.C.C.R.*, 1996, pp. 57 à 81, spéc. p. 76 note 4; *contra* mais à tort, Civ. Bruxelles (Prés.), 22 mars 1994, *op. cit.* et obs. critiques de Th. LÉONARD; Civ. Nivelles (Prés.), 15 novembre 1994, *J.T.*, 1995, p. 289; de manière plus générale sur cette problématique, voir J.-Fr. VAN DROOGHENBROEK, 'La nature et le régime de la compétence exercée comme en référé. L'exemple de l'action en dommages et intérêts', *J.T.*, 1996, p. 553 et s.
205. Th. LÉONARD, obs. sous Civ. Bruxelles (Prés.), 22 mars 1994, *op. cit.*, p. 845, n° 8.
206. Article 14, § 6 de la loi.
207. Article 14, § 7 de la loi.
208. Article 14, § 2 de la loi.

890 **Saisine de la juridiction et recevabilité de l'action**

Le Président est saisi par voie de requête contradictoire selon une procédure réglée par l'article 14 de la loi ainsi que par les articles 1034*bis* à 1034*sexies* du Code judiciaire [209].

C'est la juridiction présidentielle du domicile du requérant qui est normalement compétente territorialement [210].

L'action n'est recevable que si une demande de droit d'accès ou de rectification a été rejetée ou s'il n'y a pas été donné suite dans les quarante-cinq jours concernant la demande d'accès [211] ou dans le mois des demandes de rectification ou d'opposition [212]. Ce délai d'attente est en pratique un inconvénient important qui poussera, sans doute, à préférer une véritable action en référé aux fins d'obtenir d'urgence une décision provisoire sur les droits de la personne concernée.

Cette action a été, pour l'instant, rarement mise en œuvre [213]. Il faut rappeler ici qu'elle ne peut être introduite par le responsable du traitement lui-même. Certains ont dès lors attaqué des concurrents pour violation de la loi sur la base de l'action en cessation issue de la loi sur les pratiques du commerce [214].

209. S. Raes, 'La requête contradictoire', in *Le droit judiciaire rénové Premier commentaire de la loi du 3 août 1992 modifiant le Code judiciaire*, Bruxelles, Centre interuniversitaire de droit judiciaire, 1992, p. 85, n° 13. S'il existe une incompatibilité entre une formalité ou mention prescrite par les articles 1034*ter* à 1034*sexies*, et celle prescrite par la disposition légale particulière, il doit être donné préférence à cette dernière; P. Lemmens, 'De procedure zoals in kort geding betreffende de bescherming van de persoonlijke levensfeer', *op. cit.*, p. 5.

210. Si le requérant n'a pas de domicile en Belgique, c'est le Président du tribunal du domicile du responsable du traitement, voire du siège social de ce dernier (art. 14, § 2 de la loi).

211. Article 14, § 5 et 10, § 1er de la loi.

212. Article 14, § 5 et 12, § 3 de la loi.

213. Voir par exemple Civ. Bruxelles (Prés.), 19 décembre 2000, *Bull. ass.*, 2001, p. 266 et s. et note Ch. van Oldeneel; Civ. Nivelles (Prés.), 28 octobre 2003, *Bull. ass.*, 2004, p. 49 et s. et note Ch. van Oldeneel *Cf.* aussi J-P. Buyle, L. Lannoye, Y. Poullet, V. Willems, 'Le droit de l'informatique Chronique de jurisprudence (1987-1994)', *op. cit.*, pp. 237 et 238; deux décisions révèlent son application en matière de crédit à la consommation (Civ. Bruxelles (Prés.), 13 septembre 1995 et Civ. Bruxelles (Prés.), 12 avril 1995, *op. cit.*). Le Président du tribunal de première instance semble cependant sans compétence pour connaître d'une violation de la loi du 12 juin 1991 relative à la loi sur le crédit à la consommation qui prévoit des règles spécifiques en la matière (Th. Léonard, 'Centrales de crédit et protection de la vie privée: incertitude et insécurité juridique', *op. cit.*, pp. 64 à 68).

214. J-P. Buyle, L. Lannoye, Y. Poullet, V. Willems, 'Le droit de l'informatique Chronique de jurisprudence (1987-1994)', *op. cit.*, p. 238, n° 78; Y. Poullet, A. Cruquenaire, N. Daubies *et alii*, *Droit de l'informatique et des technologies de l'information Chronique de jurisprudence 1995-2001*, *op. cit.*, p. 172, n° 174.

Chapitre 6. Sanctions civiles, pénales et entrée en vigueur

900 Sanctions civiles

En vertu de l'article 15*bis* de la loi, lorsque la personne concernée subit un dommage causé par un acte contraire à la loi ou à son arrêté royal, le responsable du traitement est responsable du dommage ainsi causé et n'est exonéré de cette responsabilité que s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

On peut s'interroger légitimement sur la portée de cette disposition susceptible d'interprétations divergentes.

A-t-elle pour objet d'instaurer une – forme légère de [215] – responsabilité objective ayant pour conséquence de permettre au demandeur en responsabilité civile de ne pas devoir prouver une faute au sens du droit commun ? D'aucuns le prétendent, non sans précaution. L'objectivation de la responsabilité proviendrait du fait que si le responsable reste dans l'incapacité de prouver que le fait qui a provoqué le dommage ne lui est pas imputable, il endosse la responsabilité de l'acte et doit le réparer [216]. D'autres y voient dès lors plutôt un simple retournement de la charge de la preuve au bénéfice de la victime [217]. Une fois la contrariété à la loi prouvée, il reviendrait au responsable de démontrer que ce fait ne lui est pas imputable. Il reviendra à la jurisprudence de se prononcer.

910 Sanctions pénales

Le chapitre VIII de la loi prévoit un grand nombre de sanctions pénales en cas de violation de ses dispositions.

Les peines principales consistent généralement en des amendes dont le montant peut varier de 500 euros à 500 000 euros selon le délit. En cas de récidive, l'article 41, § 3 prévoit la possibilité pour le juge de prononcer au choix une amende et/ou une peine d'emprisonnement de trois mois à deux ans.

Les peines accessoires apparaissent comme particulièrement adaptées à la réalité réglementée. Elles présentent un caractère dissuasif certain au cas où le responsable du traitement est une personne morale. Ainsi, le juge pourra prononcer la confiscation des supports matériels des données qui forment l'objet de l'infraction (disquettes, bandes magnétiques, etc.) à l'exclusion des ordinateurs eux-mêmes ou de « *tout autre matériel* » [218]. Le but est ici d'éviter de bloquer l'activité de l'entreprise [219]. Les objets confisqués doivent être détruits lorsque la décision est coulée en force de chose jugée [220]. Le juge peut aussi ordonner l'effacement des données [221]. Il a encore la

---

215. Selon l'expression employée in D. De Bot, *Verwerking van persoonsgegevens*, *op. cit.*, p. 241, n° 326 et s.
216. *Ibidem*, p. 241, n° 327.
217. Y. Poullet, A. Cruquenaire, N. Daubies *et alii*, *Droit de l'informatique et des technologies de l'information Chronique de jurisprudence 1995-2001*, *op. cit.*, p. 169, n° 170.
218. Article 41, § 1er de la loi.
219. Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. Repr., sess. extr. 1991-1992, n° 413/12, p. 70.
220. Article 41, § 1er, al. 4 de la loi.
221. Article 41, § 1er, al. 1er; remarquons que « la confiscation ou l'effacement peuvent être ordonnés même si les supports matériels des données à caractère personnel n'appartiennent pas au condamné » (art. 41, § 1er, al. 2 de la loi).

possibilité d'ordonner « *l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'il détermine, aux frais du condamné* » [222].

Le responsable du traitement ou son représentant en Belgique sont civilement responsables du paiement des amendes auxquelles son préposé ou mandataire a été condamné [223].

Le juge pourra enfin interdire à la personne condamnée de gérer, personnellement ou par personne interposée, tout traitement de données à caractère personnel. La durée de cette interdiction ne peut toutefois excéder deux années [224].

Ces peines peuvent s'avérer extrêmement lourdes. L'exposé des motifs les justifiait par l'objet particulier de la législation: la défense d'un droit fondamental de l'individu [225].

Le texte des articles 38 et 39 de la loi désigne, le plus souvent [226], l'agent pénalement responsable devant la loi par l'expression « *le responsable du traitement, son représentant en Belgique, son préposé ou mandataire* ». L'imputabilité légale du responsable du traitement ou de son représentant en Belgique s'explique par le fait que la loi met expressément à leur charge la plupart des obligations découlant du système de protection. L'imputabilité du préposé paraît plus étrange. La lecture des travaux parlementaires révèle que l'ajout des termes « *préposé ou mandataire* » ne vise qu'à rencontrer l'hypothèse où le responsable du traitement est une personne morale [227].

Les poursuites pénales sur la base d'une infraction à la loi sont pratiquement inexistantes [228].

920 Entrée en vigueur

La loi telle que modifiée par la loi du 11 décembre 1998 est entrée en vigueur le 1er septembre 2001 [229].

L'article 9, § 2 de la loi a prévu une exception dans l'hypothèse où la première communication des données a eu lieu avant l'entrée en vigueur de cette disposition, soit le 1er septembre 2001. Le responsable bénéficiait alors d'un délai de trois ans pour procéder à la communication de l'information sauf s'il avait bénéficié d'une exemption à l'obligation d'information telle que prévue par la loi et par l'arrêté royal no 15 du 12 mars 1996 aujourd'hui abrogé.

---

222. Article 40 de la loi.
223. Article 42 de la loi
224. Article 41, § 2 de la loi.
225. *Doc. parl.*, Ch. Repr., sess. ord. 1990-1991, no 1610/1, p. 30.
226. Dans trois cas, l'imputabilité légale des faits incriminés est implicite. Le législateur utilise l'expression 'quiconque'. Il s'agit des violations de l'article 4, § 1er et, § 2 (régime de la collecte), des articles 21 et 22 (régime des flux transfrontières et des interconnexions de traitements) ainsi que de l'article 32 (entraves aux vérifications de la Commission ou de ses membres et experts).
227. Dans le cas où le responsable du traitement est une personne physique, voir M.-H. Boulanger, C. De Terwangne, Th. Léonard, 'La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel', *op. cit.*, p. 387, no 96.
228. Pour un exemple, voir Corr. Gand, 22 janvier 2001, *Computerrecht*, 2001, p. 263 et s.
229. *Cf.* l'article 70 de l'arrêté royal.